云计算关键领域安全指南

V2.1

云安全联盟（CSA）

2009 年 12 月

导论

本指南是云安全联盟文档《云计算关键领域安全指南》的第二版，第一版发布于 2009 年四月份，在以下地址可以下载到上述两份文档：

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (本文档英文版)
http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf (指南版本 1.0)

与第一个版本指南有所不同，第二版决定将关键指南和其它各领域的核心研究分开，每个领域的核心研究将会单独作为白皮书来发布。这些白皮书和它们的发布日期位于：
http://www.cloudsecurityalliance.org/guidance/domains/

与版本 1.0 相比，其它的变化还有- **D3: 法律和 D 4: 电子证据发现**合并到了一个新的关键域 **D3**。另外，**D6: 信息生命周期管理**和 **D14: 存储**合并到一个关键域 – **D6**， 这使得关键域的数量变为 13 个（上一个版本是 15 个）。

© 2010 云安全联盟 Cloud Security Alliance.
保留所有版权。您可以在您的计算机上下载、存储、显示、查看、打印、链接到云安全联盟的网址 www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf ，只要您遵循：(a) 指南用于个人、信息分享、非商业用户；(b) 指南不可以被以任何方式修改和变更；(c) 指南不可以被重新分发；(d) 必须保留商标、版权和其它声明。按照美国版权法合理使用条款，您可以在注明属于云安全联盟 CSA 的前提下引用指南 2.1(2009)的某些部分。

目录

导论 2
目录 3
前言 4
译者序 7
编者寄语 9
关于风险的编者按：决定何时、如何、将什么迁移进云？ 10
第一部分 云架构 13
D1: 云计算架构框架 14
第二部分：云的治理 29
D2: 治理和企业风险管理 30
D3: 法律与电子证据发现 34
D4: 合规与审计 36
D5: 信息生命周期管理 38
D6: 可移植性和互操作性 43
第三部分：云的运行 46
D7: 传统安全、业务连续性和灾难恢复 47
D8: 数据中心运行 49
D9: 应急响应、通告和补救 51
D10: 应用安全 54
D11: 加密和密钥管理 56
D12: 身份和访问管理 58
D13: 虚拟化 62
参考资料 64

Copyright © 2010 Cloud Security Alliance

前言

欢迎来到云安全联盟的“云计算关键领域安全指南”的第二个版本。云计算继续前进的步伐既带来了新的机遇，同时也带来了新的安全挑战。我们谦恭地希望给您提供指南和灵感，来支持您的业务、您的需求、同时管理新的风险。

尽管云安全联盟很有可能只是由于本指南而为人所知，但是在未来的几个月中您会看到各种各样的相关活动，包括国际章节、伙伴关系、新的研究、以及旨在努力推进我们的使命的会议活动。您可以在 网址 www.cloudsecurityalliance.org 得到我们最新的活动。

云计算安全的道路无疑是漫长的，需要全球范围内各行各业的利益相关者积极参与。但是，我们应该高兴地承认所取得的进展。我们看到：新的云安全解决方案不断出现；企业使用我们的指南来接触云服务供应商；并且就合规性和信任问题而展开的健康公开的对话在世界范围内大量涌现。还有，我们已经取得的最重要的胜利就是安全专业人士积极地参与到确保未来的活动中，而不是简单地耽于保护现在。

请继续参与这个主题，并继续与我们一道努力，以完成这一重要使命。

致礼，

Jerry Archer　　Dave Cullinane　　Nils Puhlmann
Alan Boehme　　Paul Kurtz　　Jim Reavis

云安全联盟理事会

致谢

编辑

Glenn Brunette
Rich Mogull

贡献者

Adrian Seccombe
Alex Hutton
Alexander Meisel
Alexander Windel
Anish Mohammed
Anthony Licciardi
Anton Chuvakin
Aradhna Chetal
Arthur J. Hedge III
Beau Monday
Beth Cohen
Bikram Barman
Brian O'Higgins
Carlo Espiritu
Christofer Hoff
Colin Watson
David Jackson
David Lingenfelter
David Mortman
David Sherry
David Tyson
Dennis Hurst
Don Blumenthal
Dov Yoran
Erick Dahan
Erik Peterson
Ernie Hayden
Francoise Gilbert
Geir Arild Engh-Hellesvik
Georg Hess
Gerhard Eschelbeck
Girish Bhat
Glenn Brunette
Greg Kane
Greg Tipps
Hadass Harel
James Tiller
Jean Pawluk
Jeff Reich
Jeff Spivey
Jeffrey Ritter
Jens Laundrup
Jesus Luna Garcia
Jim Arlen
Jim Hietala
Joe Cupano
Joe McDonald
Joe Stein
Joe Wallace
Joel Weise
John Arnold
Jon Callas
Joseph Stein
Justin Foster
Kathleen Lossau
Karen Worstell
Lee Newcombe
Luis Morales
M S Prasad
Michael Johnson
Michael Reiter
Michael Sutton
Mike Kavis
Nadeem Bukhari
Pam Fusco
Patrick Sullivan
Peter Gregory
Peter McLaughlin
Philip Cox
Ralph Broom
Randolph Barr
Rich Mogull
Richard Austin
Richard Zhao
Sarabjeet Chugh
Scott Giordano
Scott Matsumoto
Scott Morrison
Sean Catlett
Sergio Loureiro

Shail Khiyara
Shawn Chaput
Sitaraman Lakshminarayanan
Srijith K. Nair
Subra Kumaraswamy
Tajeshwar Singh
Tanya Forsheit
Vern Williams
Warren Axelrod
Wayne Pauley
Werner Streitberger
Wing Ko
Yvonne Wilson

译者序

云安全联盟 CSA 是在 2009 年的 RSA 大会上宣布成立的。自成立后，CSA 迅速获得了业界的广泛认可。现在，CSA 和 ISACA、OWASP 等业界组织建立了合作关系，很多国际领袖公司成为其企业成员。到截稿时，企业成员达到 33 个，名单中涵盖了国际领先的电信运营商、IT 和网络设备厂商、网络安全厂商、云计算提供商等。值得注意的是，中国领先的专业安全公司绿盟科技成为中国、乃至亚太地区第一个企业成员。相信在不远的将来，企业成员中还会出现越来越多的中国知名和新兴企业机构的身影。

自其成立起，云安全联盟发布的云安全指南及其开发成为云计算领域令人瞩目的安全活动。2009 年 12 月 17 日，云安全联盟发布了新版的《云安全指南》v2.1，代表着云计算和安全业界对于云计算及其安全保护的认识的一次重要升级。新版安全指南有以下两大鲜明特色：

特色 1： 务实，贴近当前的最新的业界实践。参加编写的数十位专家横跨学术界和各主要行业，大多在美国、欧洲、亚太和中国等的第一线工作，指南的内容较为真实地反映了最新的业界最佳实践和观点，提供了非常详详细、务实的大量建议，非常容易转化为项目的检查列表等形式，方便读者参考。

特色 2： 技术上面明确阐述了法律、电子证据发现（D3）以及虚拟化（D13）方面的建议指南，另外对于数据的可移植性和互操作性（D6）也是新版 CSA 安全指南的独特之处。这些内容在 ISO27001 或者 PCI-DSS 中或者没有要求，或者很少阐述。大家知道，信息安全相关法律和信息安全技术业界的相互沟通是当前国际范围的一个趋势和热点。例如，识别用户隐私数据和适用的法律法规符合性要求是云计算提供商的安全必修课。指南在此作出了重要的探索，将法律和电子证据发现单独列为一个域，就云服务用户在服务商选择、合约内容和签署等过程中应该注意的相关要点做了总结建议。虚拟化是云服务的基石技术，它给包括安全在内的各种 IT 流程提出了新课题。

译者相信指南将会在迅速发展的云计算服务及其安全保护中扮演非常关键的角色，将会得到越来越多的企业、机构、个人的关注、研究和采纳，用以指导云计算的相关项目。中文版项目将会有助于指南在中文读者中的普及并提升使用效率。

大家知道，此次发布的指南新版只包含 D1 和其它各域的摘要，除 D1 之外其它各域的全文将会以白皮书的形式陆续单独发布。项目组也会继续关注后续发布，也欢迎各位同仁专家学者加入我们。

应该说，指南原版的遣词造句对于英语非母语的读者来说相对复杂。和大家熟悉的 ISO 标准文件相比，不是很容易透彻理解。同时，由于多个开发小组共同开发，在术语的使用方面也没有做到完全一致。在翻译过程中，项目组在“信达雅”的原则下，尽量做到体现原作精髓，术语一致，符合当前大家所熟知的中文词汇用法。对于很难找到完全准确翻译词汇时，我们保留了原版的英文作为对照、或者没有翻译。尽管如此，我们意识到翻译稿距离完全贴切地体现原版的专业含义还有相当距离，建议读者尽可能地阅读英文原版或者对照阅读。另外，在当前中文版中，文档中所有的图和表都没有来得及翻译。

在项目组中，赵粮和裘晓峰翻译了前言、编者寄语和编者按、D1-云计算架构框架；焦婷翻译了 D2-治理和企业风险管理、D11-加密和密钥管理；郭宇翻译了 D3-法律与电子证据发现、D4-合规与审计、D6-可移植性和互操作性；石屹嵘翻译了 D5-信息生命周期管理、闻剑峰翻译了 D7-传统安全业务连续性和灾难恢复、D8-数据中心运行、D9-应急响应通告和补救、D10-应用安全；温劲翻译了 D12-身份和访问管理；裘晓峰翻译了 D13-虚拟化。由赵粮负责总稿，裘晓峰统一审校了翻译稿。

主要的翻译过程正值传统的新春佳节，项目组对家庭和亲属的理解与支持表示特别感谢。项目组在翻译过程中得到了绿盟科技和中国电信上海研究院的大力支持。感谢谷安天下对项目的支持。感谢张颖博士审阅并提出详尽的修改建议。另外，对各位业界同仁、专家学者对项目的关注、理解和支持表示感谢。对于翻译稿和原版中的错误及不当之处，欢迎各位读者和同仁不吝指教。联系方式：richard.zhaol@gmail.com

Copyright © 2010 Cloud Security Alliance

编者寄语

令人难以置信，仅仅短短七个月前，来自科技行业的各个角落的小组和个人齐心合力，发布了“云计算关键领域安全指南”的第一个版本。自发布之日起，这份重要的出版物的表现一直超出我们的期望，不断地帮助世界各地的组织作出明智的决定 - 是否、何时、以及如何采用云计算服务和技术。但在这短短七个月的时间里，我们的认知和云计算技术本身已经以惊人的速度在演进。第二个版本的设计主旨就是提供新的知识，并且在更深层次上支持这些挑战性的决策。

采用云计算是一个复杂的决策，涉及许多因素。我们希望这本指南将帮助您更好地了解需要提问什么问题、最新的建议措施、避免什么潜在的陷阱。我们通过对云计算安全的若干中心问题来重点阐述，试图给读者带来一个更为清晰的全景图。在此之前，这个图像往往过于复杂、不完整、或者过于简单。我们关注原有的十五个关键域（现集中为十三个关键域），为云计算安全探讨带来相关的背景和特异性：使我们能够超越笼统的、一般性的讨论，而交付更为深刻的、更有针对性的建议。

在我们的征途上，越来越多的行业组织、企业和个人加入我们，分享我们的使命和愿景，那就是开发和提升云计算领域的安全保障措施及最佳实践。他们的观点和见解对于创建一个均衡并公正的输出成果至关重要。

云计算仍是一个迅速变化的领域，要么保持在最前沿，要么就会落后。在这个新版本的指南中，借力于我们日益壮大并多元化的社区志愿专家，我们开发了更为详细的、更为精确的内容。但是，我们绝不能自满。正如安全专家们的长期实践一样，我们必须紧紧抓住云计算给业界带来的各种机遇，持续地发展演化我们的流程、方法和技术。这种演变对于我们不断成功地找到新的方法以提升安全执行和监视能力的效力和效率是非常关键的。

云计算并不必然比您目前的环境更为安全或更不安全，正如任何新技术一样，它会创造新的风险和新的机遇。在某些情况下，迁移到云计算的过程提供了一个机会，来重新设计较早的应用程序和基础设施，以达到甚至超过当前的安全要求。在另外一些情况下，将非常敏感的数据和应用程序迁移到一个新兴的基础设施，其风险可能超过您愿意容忍的程度。这一指南的目标不是确切地告诉您怎样、在哪里、将什么搬进云，而是为您提供切实可行的建议和关键问题，来帮助您将迁移过程在自己的条件下变得尽可能安全。

最后，我们代表云安全联盟和编辑工作组，感谢每一位志愿者为新版本的开发而奉献出的时间和努力。我们也一直不断地为团队扩展并提升相关的领域的奉献所鼓舞，我们相信他们的努力为指南切切实实地增加了价值。没有他们的努力和贡献，这份文档根本不会达到现在的水平。

一如以往，我们渴望听到您关于此新版指南的反馈建议。如果您发现本指南有帮助并愿意看到它的改进，请考虑作为成员或贡献者加入云安全联盟。

编辑
Glenn Brunette
Rich Mogull

关于风险的编者按：决定何时、如何、将什么迁移进云？

贯穿于整个指南，我们开发了大量的建议以减少采用云计算技术过程中的风险，但是，并不是对于所有的云计算部署每一个建议都是必要和切实可行的。在我们把不同工作小组的输出汇编成一个整体的编辑过程中，我们很快意识到根本没有足够的空间来提供所有可能的风险场景以及充分而细致的建议。正如可能某个关键应用程序过于重要而不宜转移到公共云供应商，也有可能某些数据由于价值过低，很少或根本没有理由对其在云迁移过程中部署全面的安全保护措施。

由于存在如此之多的不同的云部署选项 - 包括服务模式的 SPI（SPI 指的是 **S**aaS - 软件作为服务，**P**aaS – 平台作为服务，或 **I**aaS - 基础设施作为服务。这些将会在 D1 中深入解释）、公共与私有部署、内部与外部主机部署、再加上各种选项的排列组合 – 根本不可能用一个安全控制列表涵盖所有的情况。如同任何其它安全方面一样，各个组织在云迁移和安全控制选择过程中应采取以风险为本的路线。下面是一个简单的框架，以帮助评估初始云计算风险，为安全决策提供依据。

这个过程不是一个完整的风险评估框架，也不是用来决定所有安全需求的方法论。实际上，这是一个快速方法，用以在将某资产迁移到各种云计算模型时评估你的容忍度。

在云部署过程中识别资产

最简单的情况下，云支持的资产可以分为两大类：

1. 数据
2. 应用/功能/过程

这样来说，我们或者把数据搬进云里，或者把交易/处理（从某些部分功能一直到全部的应用程序）搬进云里。

在云计算体系中，数据和应用程序并不需要一定在同一地点，我们甚至可以只转移部分功能到云里，例如，我们可以把应用程序和数据布放在自己的数据中心，同时通过 PaaS 把一部分功能外包到云里。

评估云风险的第一步是要确定把什么样的数据或功能迁移进云，某些资产在项目范围逐渐扩大时有可能也会牵扯进来，它们也应该被考虑在内。数据和交易量往往会高于预期。

评估资产

下一步是确定这些数据或功能对于本组织的重要性。除非您的组织已经有现成的评估流程，否则您不必做特别详细的评估工作，但你至少需要对涉及到应用/功能/过程的敏感程度和资产的重要性有一个大致的评估。

对于每项资产，可以问下面这些问题：

1. 如果该项资产被广泛公布并广为散发，我们将会受到什么样的损害？
2. 如果云服务提供商的员工访问了该项资产，我们将会受到什么样的损害？
3. 如果该项功能或过程被外人操纵，我们将会受到什么样的损害？
4. 如果该项功能或过程没有提供预期的结果，我们将会受到什么样的损害？
5. 如果该项信息/数据被意外更改了，我们将会受到什么样的损害？
6. 如果该项资产在一段时间内无法使用，我们将会受到什么样的损害？

本质上，我们是在评估资产的机密性、完整性和可用性要求，以及如果全部或部分资产迁移到云中处理，这些安全性将会如何受到影响。这和评估一个潜在的外包项目非常类似，只是对于云计算，我们有各种部署选项以及内部模型。

将资产映射到可能的云部署模型

现在，我们应该已经对资产的重要性有所了解，下一步工作是确定我们对哪些部署模式更感兴趣。在开始寻找服务提供商之前，我们应该了解我们是否可以接受各种不同部署模型带来的风险：公共、私有、社区、或混合；还有托管场景：内部、外部、或都有。

对于资产，确定您是否愿意接受下列选项：

1. 公共。
2. 私有/内部
3. 私有/外部（包括专用或共用的基础设施）。
4. 社区。需要考虑主机的位置，潜在的服务供应商，以及其他社区成员的身份。
5. 混合。为了有效地评估可能的混合部署，您必须在心里对何处部署组件、功能和数据有个大致的架构图像。

在这个阶段，对于是否适合过渡到云、采用什么部署模型和位置来满足安全和风险要求，你应该已有一个不错的主意了。

评估可能的云服务模式和提供商

这一步的关注点是每个 SPI 层次上你能拥有的控制等级，以实现不同的风险管理要求。如果你正在评估某个云产品或服务，在此阶段您可能需要切换到更加全面的风险评估。

你的关注点应该在于每个 SPI 层次上你可用来减少风险的控制能力，如果您已经有具体要求（例如，要处理某些有监管要求的数据），可以在评估中把它们涵盖进来。

画出潜在的数据流

如果你是在评估一个特定的部署选项，请画出您的组织与云服务、客户和其它节点之间的数据流图。虽然这些步骤大多数停留在很高的层面，但是在最后决定之前，这对于了解是否能够以及如何将数据搬进、搬出云至关重要。

如果你还没有决定某个特定的产品或服务，请您勾勒出可接受列表上所有选项的大致数据流，这用以保证你作出最后决定时，你可以找出风险暴露点。

结论

您现在应该对准备云迁移的资产的重要性、风险承受能力（至少在高层次上）、哪些部署和服务方式组合是可以接受的等已经较为清楚了。并且，您还对敏感信息和业务的潜在风险暴露点有了大致的概念。

这些因素放在一起，应该可以对您评估本指南中的所有其它安全控制提供足够的背景支持。对于低价值的资产，你不需要相同水平的安全控制，可以跳过很多建议 – 例如现场检查、可发现性、复杂加密方法等。高价值的、有监管要求的资产可能带来非常细致的审计和数据保存要求。对于另外某个不受监管限制的高价值资产，您可以更多集中在技术层面的安全控制上。

受限于空间以及素材的深度和广度，本文件包含了各种安全建议的详尽清单。并非所有的云部署都需要所有可能的安全风险控制，预先花一点时间评估您的风险承受能力和潜在风险暴露将为您帮助您的组织选择最佳方案提供很好的背景支持。

第一部分 云架构

D1: 云计算架构框架

本域阐述了指南其它所有部分使用的概念框架。主要内容将集中在云计算的描述上，并特依照 IT 网络和安全专业人士的独特视角进行了裁剪，分为三个部分：：

- 整个指南所使用的术语，以保持一致的词汇。
- 保护云应用和云服务的架构层面的要求和挑战。
- 一个描述云服务和体系结构分类的参考模型。

本域的最后一节简要介绍了本指南其它域的内容。

了解本域阐述的架构框架是理解云计算安全指南其它部分的重要一步，该框架界定了其它域使用的术语和概念。

什么是云计算？

云计算（或云）是一个演化中的词汇，它描述了很多现有的计算技术和方法朝各种不同方向的发展。云将应用和信息资源与底层的用以交付它们的基础设施和机制分开。

云强化了协作、敏捷、扩展性、可用性，以及通过优化的、更有效率的计算来降低成本的潜能。

更具体地说，云描述了由“资源池”化的计算、网络、信息和存储等组成的服务、应用、信息和基础设施等的使用。这些组件可以迅速策划、置备、部署和退役，并且可以迅速扩充或缩减，提供按需的、效用计算类似的分配和消费模式。

从架构的角度来看，云和现有计算模型有什么相似、又有什么不同，这些相似和不同又如何影响网络信息安全实践中的组织、运行和技术路线的，围绕着这些问题有很多令人困惑的地方。

现在有许多定义尝试着从学术、架构师、工程师、开发人员、管理人员和消费者等不同的的角度来定义什么是云。本文件的重点是从专门针对 IT 网络和安全专业人士的独特视角来裁剪的云的定义。

我们可以用统一分类的一组公用的、简洁的词汇来描述云架构对安全架构的影响，在这个统一分类的方法中，云服务和架构可以被解构，也可以被映射到某个安全、可操作控制、风险评估和管理框架等诸多要素的补偿模型中去，进而符合合规性标准。

云计算是由什么组成的？

云安全联盟安全指南的早期版本在编写时美国国家标准技术研究院（NIST）的科学家还没有开始定义云计算。

NIST 的出版物是普遍认同的，所以，我们选择与 NIST 对云计算的工作定义（本文档写作时是版本 15）保持一致，这样我们能够集中精力到用例上，而不是细微的语法定义差别上，同时还能带来连贯性和共识。

值得注意的是，本指南的目的是使其具有广泛的易用性、适用于全球范围内的组织。虽然 NIST 是美国政府机构，选择此参考模型不应该被解释为是对其它观点或地域的排斥。

NIST 给云计算定义了五个关键特征、三个服务模型、四个部署模型。图 1 是它们很形象的总结，后面将会有详细描述。

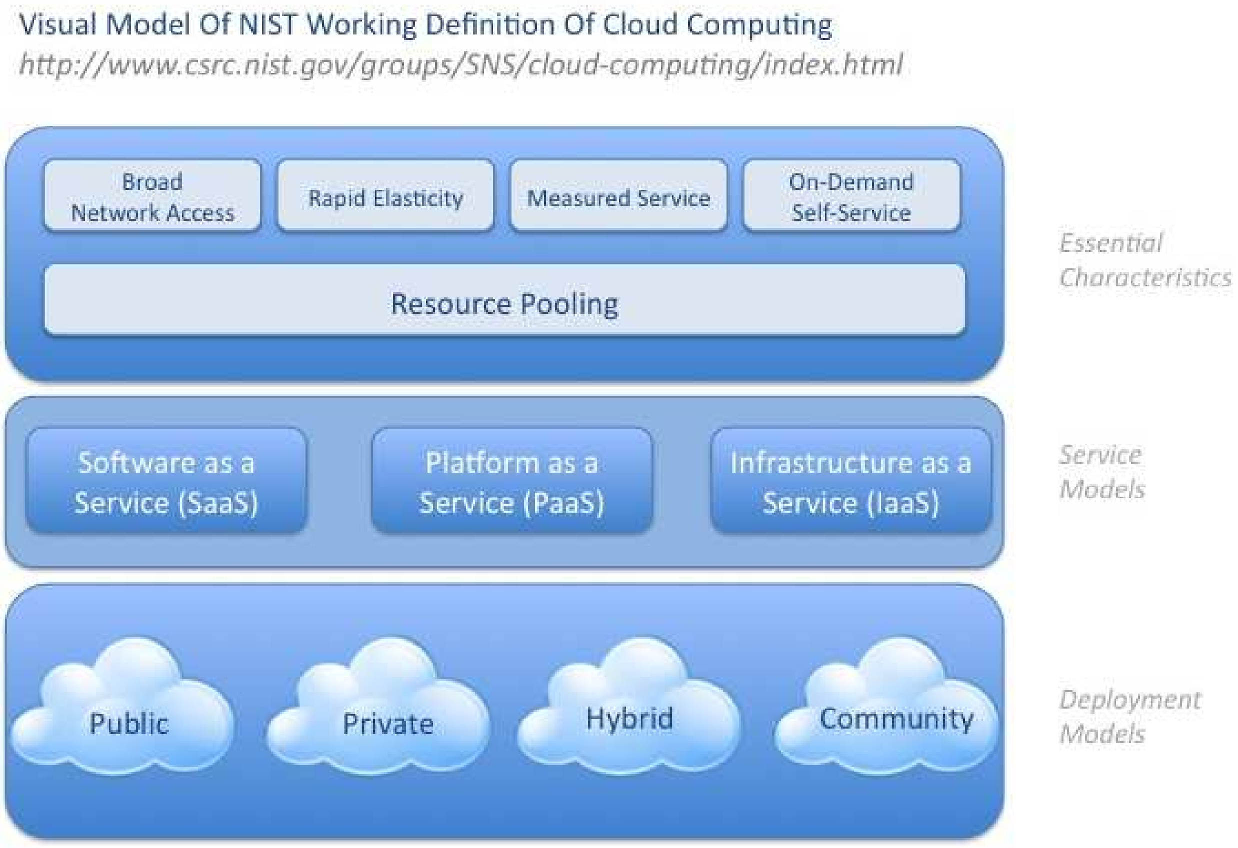


图 1 – NIST 云计算定义的形象模型

云计算的关键特征

云服务展现出的五个关键特征，代表了它与传统计算方法的关系和区别：

- **按需自服务。** 用户可以在需要时自动配置计算能力，例如服务器时间和网络存储，的需要自动计算能力，而无需与服务供应商的服务人员交互。
- **宽带接入。** 服务能力通过网络提供，支持各种标准接入手段，包括各种瘦或胖客户端平台（例如移动电话、笔记本电脑、或 PDA），也包括其它传统的或基于云的服务。
- **虚拟化的资源“池”。** 提供商的计算资源汇集到资源池中，使用多租户模型，按照用户需要，将不同的物理和虚拟资源动态地分配或再分配给多个消费者使用。虽然存在某种程度上的位置无关性，也就是说用户无法控制或根本无法知道所使用资源的确切物理位置，但是原则上可以在较高抽象层面上来指定位置（例如国家、州、省、或者数据中心）。资源的例子包括存储、处理、内存、网络带宽以及虚拟机等。即使是私有的“云”往往也趋向将资源虚拟“池”化来为组织的不同部门提供服务。
- **快速弹性架构。** 服务能力可以快速、弹性地供应 – 在某些情况下自动地 – 实现快速扩容、快速上线。对于用户来说，可供应的服务能力近乎无限，可以随时按需购买。
- **可测量的服务。** 云系统之所以能够自动控制优化某种服务的资源使用，是因为利用了经过某种程度抽象的测量能力（例如存储、处理、带宽或者活动用户账号等）。人们可以监视、控制资源使用、并产生报表，报表可以对提供商和用户双方都提供透明。

必须认识到的重要一点是虽然云服务经常和虚拟化技术一起使用，或者云服务基于虚拟化技术，但是并不必然。没有要求将资源抽象与虚拟化技术必须绑在一起。很多云服务产品并没有使用**超级监视者（hypervisor）**或操作系统容器。

进而，应该注意到，多租户并没有成为 NIST 云计算定义中的某个关键特征，但是，在讨论中被经常称为关键特征。在后面云部署模型之后的“多租户”一节可以找到更多细节。

云服务模型

云服务的交付可以分为三种模式以及不同的衍生组合。这三种基本类型经常被称为“SPI”模型，其中 SPI 分别代表软件、平台和基础设施（作为服务）。它们的定义如下：

- **云软件作为服务 (SaaS).** 提供给用户的能力是使用服务商运行在云基础设施之上的应用。用户使用各种客户端设备通过“瘦”客户界面（例如浏览器）等来访问应用（例如基于浏览器的邮件）。用户并不管理或控制底层的云基础设施，例如网络、服务器、操作系统、存储、甚至其中单个的应用能力，除非是某些有限用户的特殊应用配置项。
- **云平台作为服务 (PaaS).** 提供给用户的能力是在云基础设施之上部署用户创建或采购的应用，这些应用使用服务商支持的编程语言或工具开发，用户并不管理或控制底层的云基础设施，包括网络、服务器、操作系统、或存储等，但是可以控制部署的应用，以及应用主机的某个环境配置。

- **云基础设施作为服务 (IaaS).** 提供给用户的能力是云供应了处理、存储、网络，以及其它基础性的计算资源，以供用户部署或运行自己任意的软件，包括操作系统或应用。用户并不管理或控制底层的云基础设施，但是拥有对操作系统、存储和部署的应用的控制，以及一些网络组件的有限控制（例如主机防火墙等）。

NIST 模型和本文档并没有直接阐述代理的服务模型定义，云服务代理提供仲裁、监视、变革/移植、治理、供应和集成服务，也提供用户和各云服务商之间的谈判。

简而言之，因为创新会驱动快速的解决方案开发，云服务的用户和供应商将会喜欢与云服务交互的各种方法，像开发 API 接口什么的，所以云服务代理将会成为总体云生态环境中的重要一环。

在通用、开放、标准化的长远解决方案出台之前，云服务代理将各种不兼容的能力和接口进行抽象，为用户提供代理访问手段。所谓长远解决方案是指一种语义层面的能力，使用户流畅而灵活地充分利用最能满足自己特定需求的模型。

很重要的一点是，我们必须看到围绕着开发公开和私有的 API 方面的各种努力，这些 API 用于云的管理、安全以及互通。 简单列举几个这种 API 接口，像开放云计算接口工作组（Open Cloud Computing Interface Working Group）, Amazon EC2 API, VMware 公司 DMTF 提交的 vCloud API, Sun 公司的 Open Cloud API, Rackspace API, 以及 GoGrid’s API。 开放、标准的 API，以及通用容器格式，例如 DMTF 的开放虚拟化格式 OVF（Open Virtualization Format），它们在云可移植性和可交互性方面将会扮演至关重要的角色。

虽然当前有很多工作组、草案以及已发布的规格标准，但是肯定会出现一个整合的过程，各种市场力量、用户需求和经济环境等相互博弈、去粗存精，最后达到一个让用户更方便管理和互操作的状态。

云部署模型

不管利用了哪种服务模型（SaaS、 PaaS、或 IaaS），存在四种云服务部署模型，以及用以解决某些特殊需求而在它们之上的演化变形。

- **公共云。**由某个组织拥有，其云基础设施对公众或某个很大的业界群组提供云服务 。
- **私有云。** 云基础设施特定为某个组织运行服务。可以是该组织或某个第三方负责管理，可以是场内服务（on-premises），也可以是场外服务（off-premises）。
- **社区云。** 云基础设施由若干个组织分享，以支持某个特定的社区。社区是指有共同诉求和追求的团体（例如使命、安全要求、政策或合规性考虑等）。可以是该组织或某个第三方负责管理，可以是场内服务（on-premises），也可以是场外服务（off-premises）。
- **混合云。**云基础设施由两个或多个云（私有的、社区的、或公共的）组成，独立存在，但是通过标准的或私有的技术绑定在一起，这些技术促成数据和应用的可移植性（例如用以云之间负载分担的 cloud bursting 技术）。

在市场产品消费需求越来越成熟的过程中，将会出现其它的派生的云部署模型，意识到这一点很重要。这方面的一个例子就是虚拟专用云（virtual private clouds）- 以私有或半私有的形式来使用公共云基础设施，通常通过虚拟专网 VPN 将公共云里的资源连回用户数据中心内部的资源。

方案设计时的架构思路对将来方案的灵活性、安全性、移动性以及协作能力都有很大的影响。作为一条首要原则，“边界化（perimeterized）”的解决方案没有“去边界化（de-perimeterized）”的方案更有效，在上述四个部署模型中都这样。同样的道理，采取私有的还是开放的方案也需要仔细考量。

多租户（Multi-Tenancy ）

虽然并不是 NIST 模型中云计算的本质特性，CSA 将多租户识别为云的一个重要元素。

云服务模型中的“多租户”意味着满足不同客户场景对策略驱动的安全增强、分段、隔离、监管、服务水平以及相应的计费/返款等模型的不同需求。用户可能会使用公共云服务提供商的服务产品或者是同一家组织内部的云服务，例如不同的业务单元 BU（business unit），并不是完全不同的商业组织，它们之间依然需要分享基础设施。

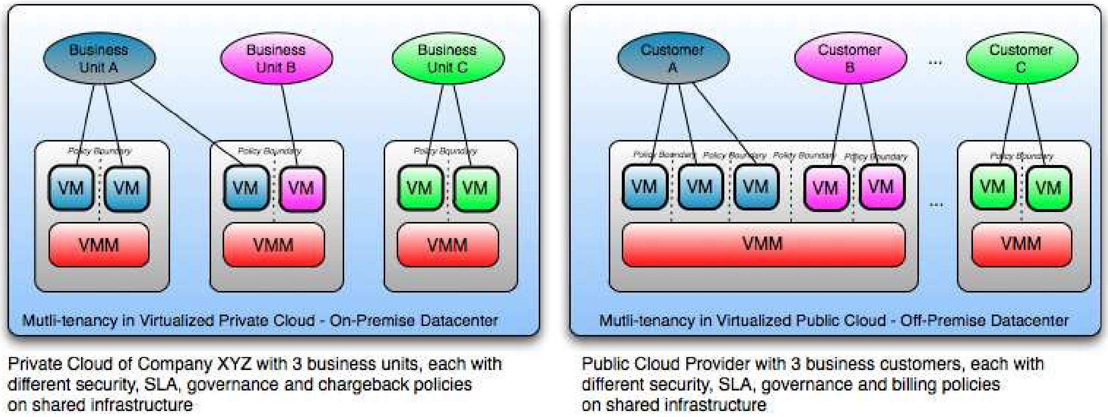


图 2 – 多租户

从提供商的角度来看，多租户对架构和设计提出的要求是通过在很多不同客户之间分享基础设施、数据、元数据、服务和应用等，来实现可扩展、可用性、管理、分段、隔离以及运行效率等方面的“经济性”。

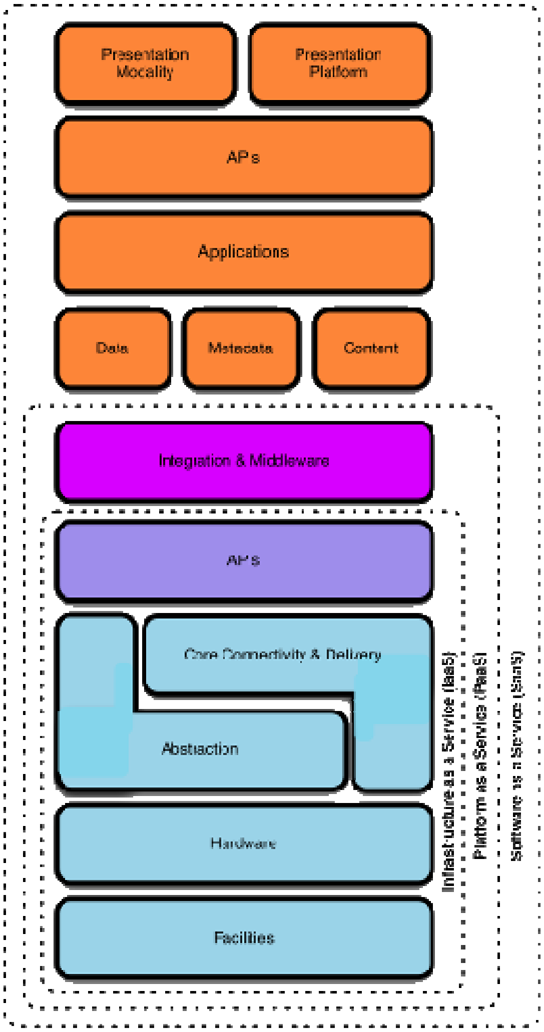


图 3 – 云参考模型

依赖于服务商的云服务模型，“多租户”也可以采用不同的定义，因为它可能与在基础设施、数据或应用等不同水平上实现的细节有关。IaaS 和 SaaS 多租户实现上的不同就是一个例子。

“多租户”在不同的云部署模型中的重要性也有所不同。然而，即使在私有云中，组织虽然只有一个，但是也存在多个来自第三方的顾问和合同工，也存在对不同业务单元间高等级逻辑分离的期望，因此，也需要考虑“多租户”。

云参考模型

理解云计算模型之间的关系和依赖性对于理解云计算的安全风险非常关键。IaaS 是所有云服务的基础，PaaS 建立在 IaaS 之上，而 SaaS 又建立在 PaaS 之上，之间关系参见云参考模型的图示。沿着这个思路，如同云服务能力是继承的那样，信息安全风险和问题也是继承的。重要的一点是，商业云提供商可能并没有与这个模型准确对应，然而，云参考模型对于将真实服务和某个架构框架联系在一起，进而理解需进行安全分析的资源和服务是非常重要的。

IaaS 涵盖了从机房设备到其中的硬件平台等

所有的基础设施资源层面。它包括了将资源抽象化（或相反）的能力，并交付连接到这些资源的物理或逻辑网络连接，终极状态是 IaaS 提供商提供一组 API，允许用户与基础设施进行管理和其它形式的交互。

PaaS 位于 IaaS 之上，又增加了一个层面用以与应用开发框架、中间件能力以及数据库、消息和队列等功能集成。PaaS 允许开发者在平台之上开发应用，开发的编程语言和工具由 PaaS 支持提供。

类似的，SaaS 又位于底层的 IaaS 和 PaaS 之上。SaaS 能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。

因此，必须清楚，在三个模型中，集成的特色功能、复杂性与开放性（可增强性）以及安全等方面会有一些明显的折中。三种云部署模型之间的折中包括：

- 一般来说，SaaS 会在产品中提供最为集成化的功能 ，最小的用户可扩展性（extensibility），相对来说较高的集成化的安全（至少提供商承担安全的职责）。
- PaaS 提供的是开发者在平台之上开发自己应用的能力。因此，它倾向于提供比 SaaS 更多的可扩展性，其代价是 SaaS 那些已经用户可用的特色功能。这种折中也会延伸到安全特色和能力上，虽然内置的安全能力不够完备，但是用户却拥有更多的灵活性去实现额外的安全。
- IaaS 几乎不提供那些和应用类似的特色功能，但却有极大地“可扩展性”。这一般是指 IaaS 在除了保护基础设施自身之外的安全保护能力和功能更少。IaaS 模型要求云用户自己管理和安全保护操作系统、应用和内容。

云安全架构的一个关键特点是云服务提供商所在的等级越低，云服务用户自己所要承担的安全能力和管理职责就越多。

在 SaaS 情况下，这意味着在合同里需要对服务本身和提供商的服务水平、安全、管控、合规性以及责任期望等有明确要求。在 PaaS 或 IaaS 情况下，这些内容的管理责任是用户自己的系统管理员，提供商对于安全保护底层平台和基础设施组件以确保基本服务的可用性和安全，其具体要求可能会有一些相关的出入。很明确的一点是用户可以指定/转移责任（responsibility），但不一定非要指定/转移可纠责性（accountability）。

如果将每种云交付模型的范围或具体能力/功能，或它们相互交叉耦合的一些功能缩小一下，将会产生很多衍生的分类。例如存储作为服务（Storage as a Service）就是 IaaS 家族中的一个具体的子服务。

云计算的解决方案正在不断地演进，虽然讨论它的全景图超出了本文档的范围，但下面这张 OpenCrowd Cloud Solutions 分类图还是给出了一个非常不错的起点，它展示了当前风起云涌的由上述几种部署模型衍生而来的种种云解决方案。

应该注意到，CSA 并不特别支持下图所列出的任何解决方案，而只是用来说明当前市场上提供的云解决方案的多样性。

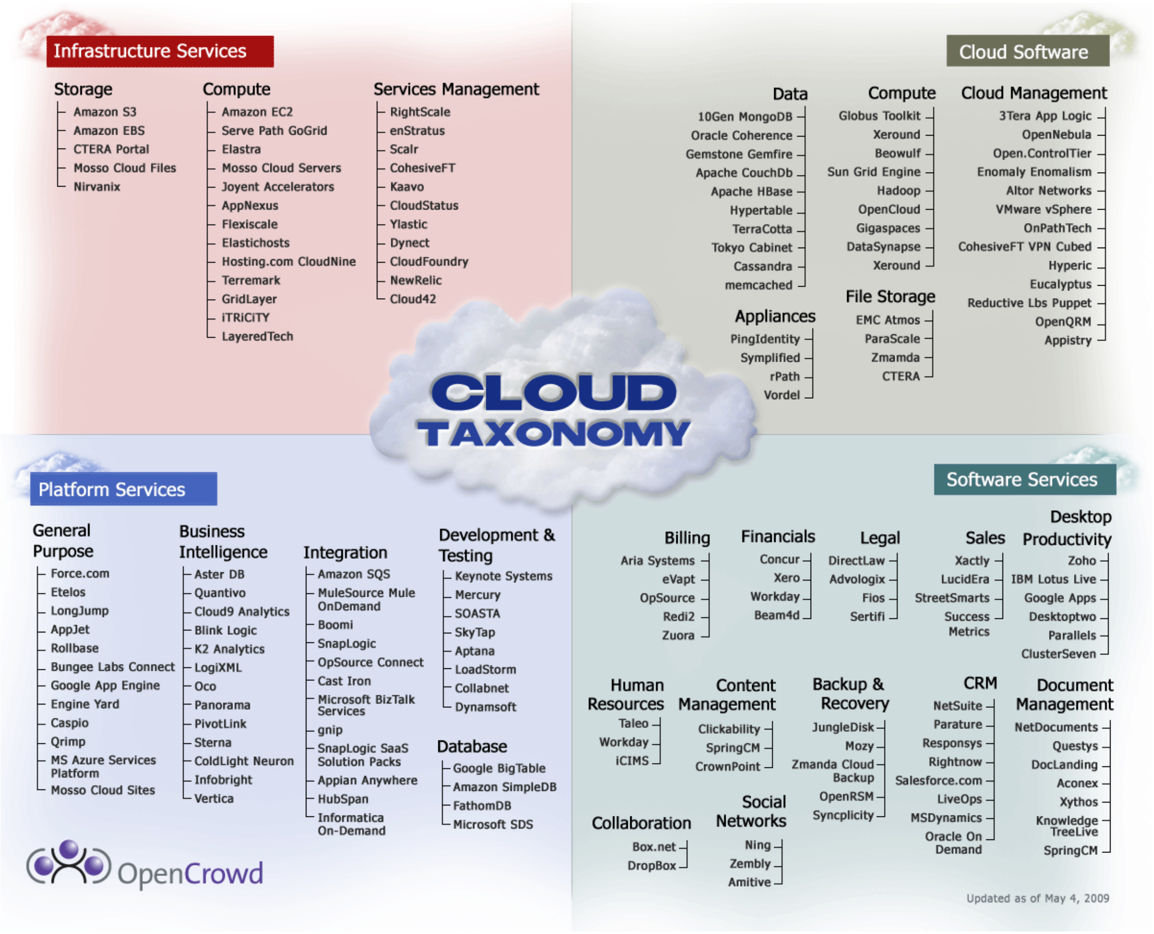


图 4 - OpenCrowd 分类图

为了提供一个云计算用例的全面视图，Cloud Computing Use Case Group 开发了一个协同任务来描述和定义通用案例并展示云带来的好处，他们的目标设定为：“...让云用户和提供商一起来定义云计算的公共用例…强调云计算环境中需要标准化的能力和要求，以确保互操作性、更易集成、可移植性。”

云安全参考模型

云安全参考模型解决的是这些分类的关系，并把它们和与其相关的安全控制和顾虑放在一个上下文环境中。对于头一次接触云计算的组织和个人来说，注意到下面的问题以避免潜在的陷阱和困惑是很重要的：

1. 云服务是如何部署的”与“云服务是在哪里提供的”这样的概念频繁混用所带来的困惑。例如，公共或私有可能被描述成外部或内部云，这种互换不是所有情况下都是准确的。
2. 云服务的使用方式经常被描述成与组织的管理或安全边界位置有关（通常定义在某个防火墙上）。虽然了解云计算中安全边界在哪里很重要，但是，“界限清晰的边界”的这一概念是一个时代性错误。
3. 在企业中正在上演的对信任边界的重组（re-perimeterization）及侵蚀，被云计算放大并加速。无处不在的连接、各种形式的信息交换、无法解决云服务动态特性的传

统静态安全控制，这些都要求针对云计算的新思维。针对企业网络的边界重整，Jericho Forum 开发了相当多的材料，包括很多案例分析。

云的部署和消费模式不能仅仅在“内部”还是“外部”上讨论，因为它们只是与资产、资源和信息的物理位置有关，而是还要讨论由谁消费、谁负责监管、安全和政策标准的合规等。

这里不是在建议某个资产、资源和信息是在“场内”（on-premise）还是“场外”（off-premise）对组织的安全和风险状态没有影响，它们的的确确有影响。但是，这里更想强调的是风险还与这些有关：

- 所要管理的资产、资源和信息类型
- 谁管理？如何管理？
- 选择了哪些控制？如何集成？
- 合规性问题

例如，Amazon AWS EC2 里部署的 LAMP 套件应该分类为公共的、场外的、第三方管理的 IaaS 解决方案，即使其中的实例、应用、数据是由消费者或某个第三方负责管理。部署在 Eucalyptus 的某个常规应用，为若干个业务单元服务，由某个公司控制、管理并拥有，可以分类为私有的、场内的、自管理的 SaaS 解决方案。两个例子都使用了云的弹性架构和自服务能力。

下面的表格总结了这些要点：

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc...
[2] Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
[3] Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control
[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

表 – 云计算部署模型

另外一个将云服务模型、部署模型、资源物理位置、管理和所有者属性等图形化展示的方法是 Jericho Forum （www.jerichoforum.org）的云立方体模型（Cloud Cube Model），如下图所示：

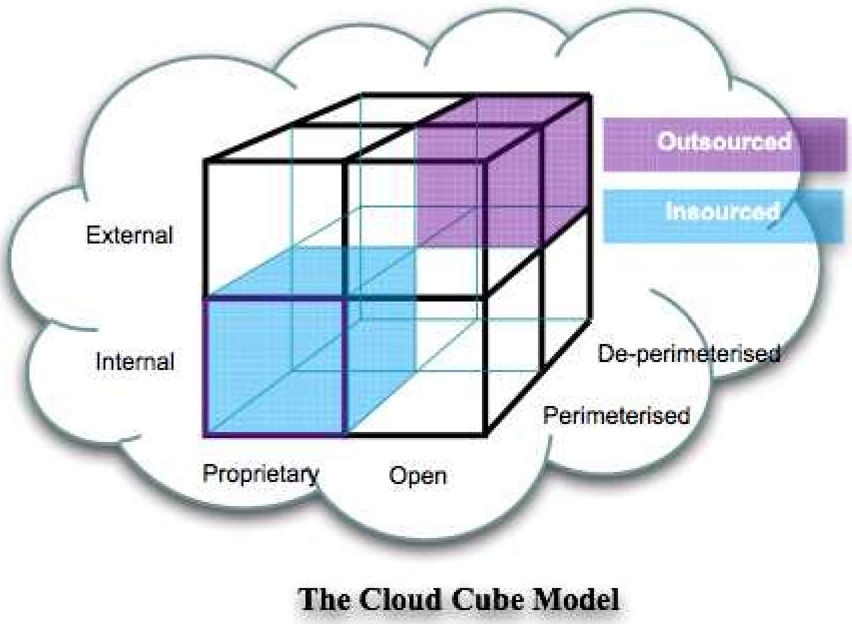


图 5 - Jericho 云立方体模型

云立方体模型很形象地阐述了市场上现有云产品的各种排列组合，提出了用以区分云从一种形态（formation）转换到另外一种形态的四种准则/维度，以及各种组成的供应配置方式以便理解云计算影响安全路线的方式。

云立方体模型还凸显了在理解云模型并将云模型映射到控制框架和标准上去时的挑战，这些控制框架和标准，像 ISO/IEC27002，提供了“一系列指南和通用原则，用以在组织内部启动、部署、维护和提升信息安全管理”。

在 ISO/IEC 27002 的 6.2 节，“外方”（External Parties）控制目标有:“… 组织的信息和信息处理设施的安全不应该因为引入外方产品或服务而降低 …”

因此，三种云服务模型的安全防护在方法和责任上有所不同，这意味着云服务的消费者面临很有挑战性的工作。除非云提供商愿意透露自己的安全控制以及为消费者部署的程度，同时消费者也知晓自己需要哪些控制以保持信息安全，否则，肯定会有可能出现大量的误导下的决策并损失惨重。

这很关键。第一是针对云架构模型对云服务分类。接下来是映射其安全架构，以及业务、监管和其它合规要求；与其相对的是一个差距分析练习。输出的结果决定了某个云服务的一般“安全”状态，以及它如何和某个资产的保障保护要求关联到一起。

下图给出了一个很好的例子说明，如何通过对云服务组件和安全控制策略集的映射来确定哪些安全控制是存在或缺失的，这些安全控制分别由客户，云服务提供商或第三方提供。这也可以与合规框架或者强制要求（如 PCI DSS）来进行比较，同样如下图所示。

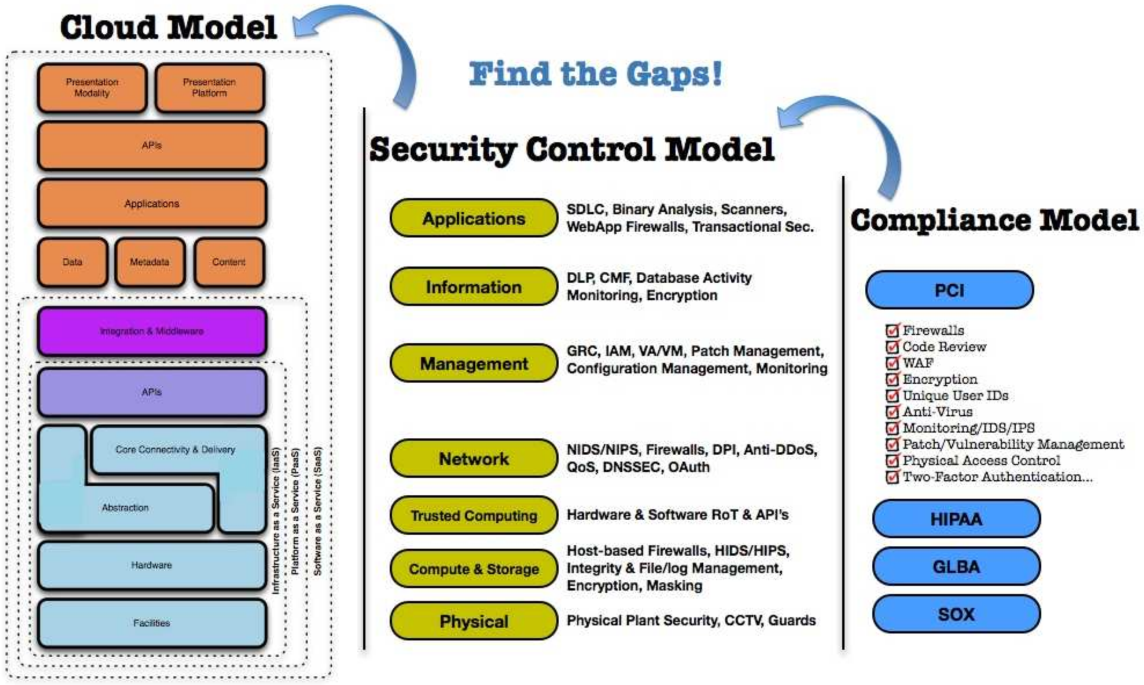


图 6 – 云模型、安全控制和合规模型的映射

完成差距分析后，按照监管方和合规方面的要求，决定需要做哪些以填入风险评估框架就容易多了。相应地，这也可以帮助决定如何对待这些安全“差距”或最终的风险 – 接受、转移、或降低。

需要意识到的重要一点是，使用云计算作为一种运行模型并不会自然地提供或妨碍达成合规性。对于任何要求的合规是服务、所使用的部署模型、以及对范围内的资源的设计、部署、管理等的直接结果。

下面是几个对控制框架非常好的全面总结，它们提供了上面提及的通用控制框架的精彩阐述，包括开放安全架构小组（Open Security Architecture Group）的安全架构模式文档，还有最近刚刚更新的 NIST 800-53 revision 3 - Recommended Security Controls for Federal Information Systems and Organizations.

什么是云计算的安全？

云计算中的安全控制其主要部分与其它 IT 环境中的安全控制并没有什么不同，然而，基于采用的云服务模型、运行模式以及提供云服务的技术，与传统 IT 解决方案相比云计算可能面临不同的风险。

即使有些运行责任落在某个或某些第三方伙伴身上，云计算的一个独特点就是能够在适度地失去控制的同时又能保持可纠责性（accountability）。

一个机构的安全态势的特征取决于成熟度、有效性以及实现基于风险调节的安全控制的完全程度，这些安全控制可以在一层或多层上实现，包括设备（物理安全）、网络基础设施（网络安全）、IT 系统（系统安全），一直到信息和应用（应用安全），更多的控制还包括人员和过程层面的，职责分离和变更的管理等。

本文前面已提到，在不同云服务模型中，提供商和用户的安全职责有很大的不同。例如，Amazon 的 AWS EC2 架构作为服务包括了一直到 hypervisor 安全的供应商的安全责任，也就是说它们只能解决物理安全、环境安全和虚拟化安全这些安全控制，而用户则负责与 IT 系统（事件）相关的安全控制，包括操作系统、应用和数据。

Salesforce.com 的客户资源管理 CRM SaaS 提供的正好相反，因为整个“栈”都由 Salesforce.com 提供，提供商不仅负责物理和环境安全还必须解决基础设施、应用和数据相关的安全控制，这减轻了用户的许多运行责任。

云计算的吸引力之一在于由经济上的可扩展性、重用和标准化提供的成本效率，为了支撑这种成本效率，云提供商提供的服务必须足够灵活，以服务最大可能的用户数、最大化他们的市场，不幸的是，将安全集成到这些服务方案中常被认为使得方案变得僵化。

这种僵化常与传统 IT 相比，表现在云环境不能部署同等的安全控制，这主要是由于基础设施的抽象化、缺少可视化、缺少集成多种熟悉的安全控制手段的能力，特别是在网络层上。

下图表明了这些问题：在 SaaS 环境中，安全控制及其范围在服务合同中进行协商；服务等级、隐私和符合性等也都在合同中关系到。在 IaaS 中，低层基础设施和抽象层的安全保护属于提供商职责，其它职责则属于客户。PaaS 则居于两者之间，提供商为平台自身提供安全保护，平台上应用的安全性及如何安全地开发这些应用则为客户的职责。

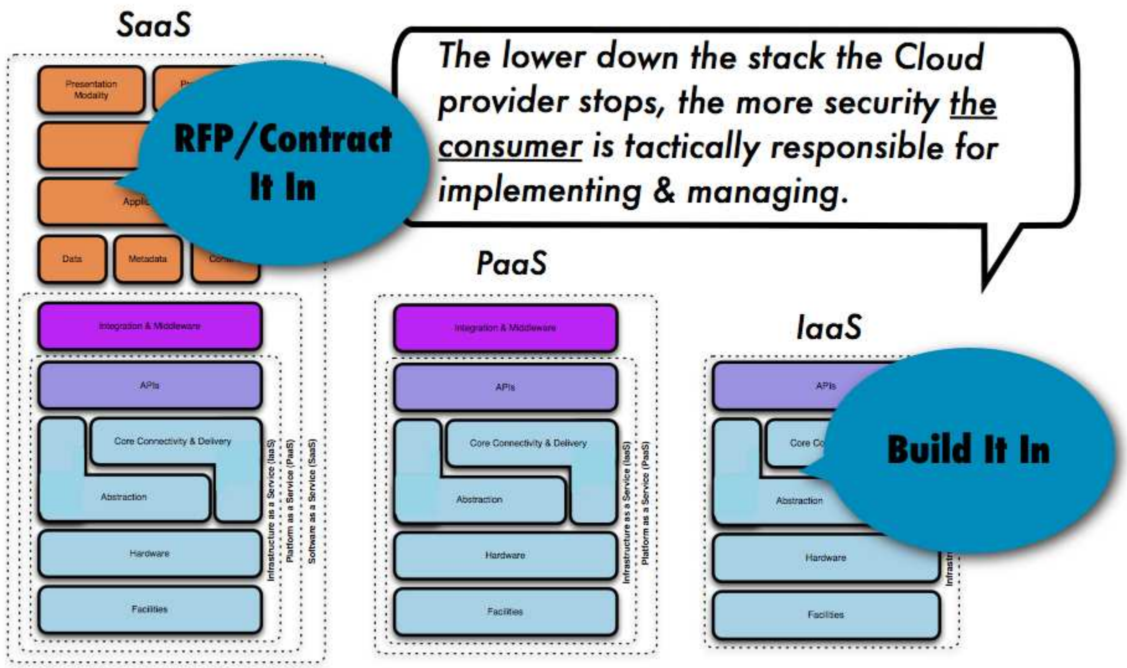


图 7 - 安全是如何集成的

理解不同服务模型间的这些不同带来的影响，以及如何进行部署对于管理企业面对的风险是至关重要的。

架构之上：关键关注领域

组成 CSA 指南的其它１２个域突出了对云计算安全的关注领域，并特别设法去解决云计算环境中战略和战术安全的“痛处”（pain points），从而可应用于各种云服务和部署模式的结合。

这些域分成了两大类：治理（governance）和运行。治理域范畴很宽，解决云计算环境的战略和策略，而运行域则关注于更战术性的安全考虑以及在架构内的实现。

治理域

域	指南解决的问题…
治理和企业风险管理	机构治理和评测云计算带来的企业风险的能力。例如违约的司法惯例、用户机构充分评估云提供商风险的能力、当用户和提供商都有可能出现故障时保护敏感数据的责任、国际边界对这些问题有何影响等都是讨论的一些问题。
法律和电子证据发现	使用云计算时可能的法律问题。本部分关系到的问题包括信息和计算机系统的保护要求

	、安全性被破坏时的披露法律、监管要求、隐私要求和国际法等。
合规性和审计	这部分考虑保持和证实使用云计算时的合规性，包括评估云计算如何影响内部安全策略的合规性、以及不同的合规性要求（规章、法规等）。这个域还包括通过审计证明合规性的一些指导。
信息生命周期管理	以下这些问题将在这部分讨论：管理云中的数据，包括与身份和云中的数据控制相关的项；可用于处理数据搬移到云中时失去物理控制这一问题的补偿控制；其它项，如谁负责数据机密性、完整性和可用性等
可移植性和互操作性	将数据或服务从一个提供商搬移到另一个提供商，或将它全部搬移到本地的能力。提供商间互操作性相关的问题也在这里讨论。

运行域

传统安全、业务连续性和灾难恢复	云计算如何影响当前用于实现安全性、业务连续性和灾难恢复的操作处理和规程，主要关注点是讨论和检查云计算的潜在风险，希望增加对话和讨论以解决令人生畏的企业风险管理模型的提升需求。进而，本节还讨论了如何帮助人们识别云计算在什么地方可以有助于减少安全风险，在某些其它领域则增加了风险。
数据中心运行	如何评估提供商的数据中心架构和运行。主要关注在帮助用户识别对于后面服务不利的数据中心特征，以及有助于长期稳定性的基础特征。
事件响应、通告和补救	适当的、充分的事件检测、响应、通告和补救。尝试解决为了启动适当的事件处理和事后分析机制，在用户和提供商两边都需要就绪的一些条目。本域将会帮助您理解云给您现有的事件处理程序带来的复杂性。
应用安全	保护在云中运行或即将开发的应用。包括将某个应用迁移到或设计进云中运行是否适当，如果适当，什么类型的云平台最适当（SaaS, PaaS, or IaaS）。还讨论了一些跟云有关的具体安全问题。
加密和密钥管理	识别恰当使用加密以及可扩充规模的密钥管理的方法。本节并不是什么规定，而是侧重

	提供信息，为什么需要这些方法，识别使用过程中出现的问题，包括保护对资源的访问以及保护数据。
身份和访问管理	利用目录服务来管理身份，提供访问控制能力。关注点是组织将身份管理扩展进云中遇到的问题。本域提供了就评估组织实施身份访问管理 IAM 的就绪性的一些见解。
虚拟化	虚拟化在云计算中的应用。本域关系到与多租户、VM 隔离、VM 共居（co-residence）、hypervisor 脆弱性等相关的项。特别关注于系统和硬件虚拟化相关的安全问题，而不是对各种形式的虚拟化的综述。

综述

通用简洁的词汇是理解云架构如何影响安全架构的关键，这些词汇又与市场上云产品的分类相关。通过云产品分类，云服务、云架构可以被解构，映射到某个安全和运行控制模型、风险评估框架、管理框架、相应的合规性标准等。

在部署云计算模型时，理解架构、技术、流程和人力资本如何变化、或者保持不变非常关键。如果对较高架构层面上的影响没有清楚的理解，就不可能理性地解决那些细节问题。

和其它 12 个关键域一道，这个架构总揽将会带给读者一个扎实的基础，就云计算环境中的安全进行评估、运行化（operationalizing）、管理、治理等。

贡献者: Glenn Brunette, Phil Cox, Carlo Espiritu, Christofer Hoff, Mike Kavis, Sitaraman Lakshminarayanan, Kathleen Lossau, Erik Peterson, Scott Matsumoto, Adrian Seccombe, Vern Williams, Richard Zhao

第二部分：云的治理

D2: 治理和企业风险管理

在云计算中，有效地治理和企业风险管理是从良好开发的信息安全治理过程得到的，是组织的全面企业治理责任应有的注意(due care)。良好开发的信息安全治理过程会使信息安全管理程序一直可依据业务伸缩、可在组织内重复、可测量、可持续、可防御、可持续改进且具有成本效益。

云计算中的治理和企业风险管理的基本问题关系到识别和实施适当的组织架构、流程及控制来维持有效的信息安全治理、风险管理及合规性。组织还应确保在任何云部署模型中，都有适当的信息安全贯穿于信息供应链，包括云计算服务的供应商和用户，及其支持的第三方供应商。

治理建议

√ 一部分从云计算服务节省的费用必须投资到提升提供商的安全能力、应用的安全控制和正在进行的详细评估和审计检查中，以确保能够持续满足需求。

√ 不管是什么服务或部署模型，云计算服务的用户和提供商都应开发健壮的信息安全治理。信息安全治理应由用户和提供商协作来达到支持业务使命和信息安全程序的一致目标。服务模型可以调整协同信息安全治理和风险管理中定义的角色和职责（基于各自对用户和提供商的控制范围），部署模型可能定义责任和预期（基于风险评估）。

√ 用户组织应包括审查具体的信息安全治理架构和流程，及具体的信息安全控制，作为未来提供商组织的部分应有的责任（due diligence）。应该评估提供商的安全治理流程和能力的充足性、成熟度及与用户信息安全管理流程的连续性。提供商的信息安全控制应基于风险确定并清晰地支持这些管理流程。

√ 用户和提供商间的协同治理架构和流程是很必要的，既是部分服务交付(services delivery)的设计和开发，也是风险评估和风险管理协议，然后作为服务协议的一部分。

√ 在建立服务水平协议（SLA）及合同契约义务时应包括安全部门，来确保安全需求在合同层面上是可强制执行的。

√ 在迁移进云端前，测量绩效和信息安全管理有效性的指标体系和标准都应建立起来。至少，组织应理解并文档化他们当前的指标，及运营迁移进云时，这些指标会如何变动，因为云提供商可能使用不同的（有可能不兼容）指标。

√ 只要有可能，所有服务水平协议（SLA）和合同中都应该包含安全指标和标准（尤其是那些法律和合规性需求相关的）。这些标准和指标应是文档记录的并是可证明的（可审计）。

企业风险管理建议

和任何新业务流程一样，遵循风险管理的最佳实践很重要。实践应该与云服务的具体用途相匹配，这些用途可能从无意的和临时的数据处理到处理高敏感性数据的关键业务流程。对企业风险管理和信息风险管理的全面讨论超出了本指南的范畴，以下列举了一些云特有的建议，可以整合进已有的风险管理和流程。

√ 由于许多云计算部署中缺少对基础设施的物理控制，因此与传统的企业拥有基础设施相比，服务水平协议(SLA)、合同需求及提供商文档化在风险管理中会扮演更重要的角色。

√ 由于云计算中的按需提供和多租户特点，传统形式的审计和评估可能并不适用，或需要更改。例如，一些提供商限制脆弱性评估和渗透测试，而其他的则限制提供审计日志和实时监控数据。如果这些在内部策略中都是要求的，那么就需要寻找替代的评估方法、某些具体的合同免责条款，或寻找与风险管理需求更一致的替代提供商。

√ 至于对组织的关键功能使用云服务，风险管理方法应该包括识别和评估资产、识别和分析威胁和弱点及其对资产（风险和事件场景）的潜在影响、分析事件/场景的可能性、管理层批准的风险接受水平和标准、多种风险处置（控制、避免、转嫁、接受）计划的开发。风险处置计划的结果应作为服务合约的一部分。

√ 提供商和用户的风险评估方法应一致，影响分析标准和可能性定义也一致。用户和提供商应共同开发云服务的风险场景，这应该固化在提供商为用户服务的设计中和用户的云服务风险评估中。

√ 资产清单应盘点支持云服务且在提供商控制下的资产。用户和提供商的资产分类和评估方案（evaluation scheme）应一致。.

√ 提供商及其服务都应该是风险评估的主题。云服务的使用、使用的特定服务和部署模型，都应该与组织的风险管理目标及业务目标一致。

√ 如果提供商不能演示证明其服务的全面有效的风险管理流程，用户应详细评估该供应商，以及是否可以使用用户自身的能力来补偿潜在的风险管理差距。

√ 云服务的用户应询问管理层对云服务的风险容忍和可接受的残余风险是否已经有所定义。

信息风险管理建议

信息风险管理（IRM）是将暴露(exposure)与风险联系的法则，也是通过数据所有者的风险容忍对其进行管理的能力。如此，对于设计用以保护信息资产的机密性、完整性和可用性（CIA）的信息技术资源，信息风险管理是最优先的决策支持方法。

√ 采用风险管理框架模型来评估 IRM，用成熟模型来评估 IRM 模型的有效性。

√ 建立适当的合同需求和技术控制，来收集信息风险决策所需要的数据（例如，信息使用、访问控制、安全控制、位置等）。

√ 在开发云计算项目需求前，采用用以确定风险暴露的流程。虽然了解暴露和管理能力所需的信息类别比较一般化，但实际收集的指标对于云计算 SPI 模型是特定的，是可以按照服务来采集的。

√ 在使用 SaaS 时，绝大多数信息都由服务提供商提供。组织应在 SaaS 服务合同责任中制定分析信息的收集流程。

√ 当采用 PaaS 时，建立类似上述 SaaS 服务的信息采集能力。在可能的地方，包括进部署和从控制中采集信息的能力，建立对这些控制的有效性进行测试的合同条款。

√ 当使用 IaaS 服务提供商时，在合同中为风险分析需求信息“植入”信息透明性。

√ 云服务提供商应包括指标和控制来帮助用户实施他们的信息风险管理需求。

第三方管理建议

√ 用户应该将云服务和安全视为供应链安全问题。这意味着在尽可能的程度上检查和评估提供商的供应链（服务提供商的关联和依赖关系）。这也意味着检查提供商自己的第三方管理。

√ 对第三方服务提供商的评估应具体指向提供商在事件管理、业务连续性和灾难恢复等方面的策略、流程和规程；还应包括对共用场地（co-location）和备份设施的审查。这应包括审查提供商是否遵从其自身策略和规程的内部评估，评估提供商在这些领域为其控制的绩效和有效性提供信息的指标体系。

√ 用户的业务连续性和灾难恢复计划应包括提供商服务失效的场景，及提供商的第三方服务和第三方服务依赖能力的失效场景。对计划中这部分的测试应与云提供商协调。

√ 对提供商的信息安全治理、风险管理和合规结构及流程的全面评估应包括：

- 要求文档清晰记录如何评估设施和服务的风险、审计控制弱点、评估频率及如何及时消减控制弱点。
- 要求定义提供商认为的关键服务和信息安全成功因素、关键绩效指标 KPI，及如何测量这些与 IT 服务和信息安全管理相关的内容。
- 审查提供商的法律、法规、行业及合同需求的获得、评估及沟通流程是否全面。
- 对整个合同或服务条款做尽职调查（due diligence）来确定角色、职责和可纠责性。确保法律审查，包括评估在国外或州司法管辖之外的地区当地合同条款和法律是否可以强制执行。

- 定义应有的职责(due diligence)需求是否包括了所有云提供商关系的重大方面，例如提供商的财政状况、名誉（如参考检查）、控制、关键人员、灾难恢复计划和测试、保险、通信能力及转包商的使用。

贡献者: Jim Arlen, Don Blumenthal, Nadeem Bukhari, Alex Hutton, Michael Johnson, M S Prasad, Patrick Sullivan

D3: 法律与电子证据发现

云计算的产生使组织和其信息之间出现了新型的动态关系，关系到了出现的第三方：云提供商。这也对将法律应用到广泛的信息管理场景中提出了新的挑战。

云计算相关的法律问题的完整分析应该考虑功能、司法和合同这几方面的问题。

- 功能方面主要包括确定云计算中的功能和服务，杜绝因此产生参与者和利益相关者（stakeholder）的法律问题。
- 司法方面主要包括政府管理法案和制度对于云计算服务、利益相关者和数据资产的影响。
- 合同方面主要包括合同的结构、条件和环境，以及云计算环境中的 Stakeholder 解决和管理法律和安全问题的实施办法。

总体来说，云计算和传统的外包服务有三点显著区别：服务时间（按需服务和间歇服务）、匿名服务提供商和未知的服务器所在地。特别是 IaaS 和 PaaS 这两种模式，大量的设计（orchestration）、配置以及软件开发的工作实际是由消费者自行完成的 - 很多的任务是无法由云提供商所完成的。

近年来，相对于传统的内部式或外包式架构，世界范围内法律和管理对合规的需求使得法律人士和技术专家需要更密切的配合，这一点在云计算中显得尤为突出，原因在于云特有的分布式生态环境产生了潜在的法律风险。

很多美国和欧盟的合规法律和制度将合规责任转移给分包商，或者要求商业实体通过合同进行限制。

法律界现在开始意识到信息安全管理服务是电子信息是否能被接受作为证据的关键因素。当然这是传统 IT 架构的问题，对其特别关注的原因是法律界对于云没有相关的经验。

建议

√ 在电子证据发现方面，用户和云提供商必须对对方的角色和责任有共同的认识，包括诉讼保留、发现搜索、专家证词提供方等等。

√ 建议云提供商提供真实可靠的数据，以保证他们的信息安全系统可以响应客户的要求，比如类似元数据和日志文件的主要和次要信息。

√ 云服务提供商保存的数据必须接受与在数据所有者处保存时同样级别的监管。

√ 提前计划意料内和意料外关系终止后的合同协商事宜，并有序地恢复或处置资产的安全。

√ 云服务用户的责任包括合同前尽职调查、合同期限的谈判、合同执行后的监测、合同终止、以及数据保管变更等。

- √ 实施安全策略以满足当地法规对跨边界数据流合规要求的先决条件，是了解云服务提供商数据存贮的地点。

- √ 作为个人数据或企业知识产权资产的保管者，采用云计算服务的企业应该保证该数据以原始的、可认证的格式保存所有者信息。

- √ 包括数据泄露在内的大量的安全事件，应该用服务协议的方式解决，云提供商和客户应该分别声明各自的承诺条款。

- √ 云提供商和用户应该对回应传票、服务过程和其他法律要求有统一的流程。

- √ 云服务协议必须允许云服务客户或者指派的第三方来监控服务提供商的效率，并测试系统的脆弱性。

- √ 云服务协议约定的各方应提前约定在合约关系终止后客户数据的恢复事宜。

贡献者: Tanya Forsheit, Scott Giordano, Francoise Gilbert, David Jackson, Peter McLaughlin, Jean Pawluk, Jeffrey Ritter

D4: 合规与审计

随着云计算逐渐发展成为一种可行的且具有高性价比的整体系统、甚至整体商业流程外包方式，如何通过执行安全策略和相关法规，来保持组织自身的合规性已经成为一个课题，并且变得越来越困难，特别是如何演示给审计者和评估者更是一个难题。

目前 IT 技术相关的法律法规在编写时大多没有将云计算考虑在内。通常情况审计者和评估者可能对云计算不熟悉，有时候也许使用过特定的云服务。基于以上情况，云的消费者需要理解以下几点：

- 使用特定云服务时的监管法规适用性
- 云提供商和消费者在合规责任上的区别
- 云提供商提供合规所需资料的能力
- 云消费者需要协助云提供商缩小和审计者/评估者之间的差异.

建议

√ 引入法律和合同团队。 云提供商的标准服务可能无法满足你的合规需求；因此法律和合同团队的早期介入对于保证云服务合同条款满足合规和审计要求是有好处的。

√ 审计条款的权利。 由于云和管理环境的动态变化特点，消费者经常需要审计云提供商的能力。特别是当云消费者有合规责任时，审计合同条款的权利应该可以随时获得。随着云提供商获得了相关的认证，这种需求应该会逐渐减少，稍后我们会介绍 ISO/IEC 27001 认证的相关内容。

√ 分析合规的范围。 对于给定的应用和数据，确定组织遵守的合规条例是否会受到使用云服务的影响。

√ 分析合规条例对数据安全的影响。 潜在的云服务消费者应该考虑哪种应用和数据适合以云服务的形式提供，以及这种服务合规的范围。

√ 审核相关的合作伙伴和服务提供商。 这是保证服务提供商不会对合规起负面作用的基本指导。基础的做法是，评估那些处理有合规性要求的数据的服务提供商，进而评估这些服务提供商的安全控制手段。有些合规性法规对如何访问和管理第三方厂商风险有专门的说明。对于那些没有在自身 IT 和业务服务中采用云架构的组织，也需要了解其云业务合作伙伴在处理数据时是否遵从合规性法规。

√ 理解合同中的数据保护责任和相关的合同。 云服务模型要求，消费者或者是云服务提供商都有责任部署安全控制策略。相对于 SaaS（软件即服务）来说，IaaS（基础架构即服务）场景中的消费者具有较高的控制度和责任。 从一个安全控制标准点来看，这意味着 IaaS 的消费者将需要为合规部署很多安全控制点。在 SaaS 场景中，云服务提供商必须提供必需的（安全）控制。从合同的角度来看，理解特殊的需求，并保证云服务合同和服务水平协议（SLA）可以最终解决合规性的问题。

- √ 分析合规条例对提供商基础架构的影响。 将基础架构迁移到云服务上同样需要慎重的分析。某些管理要求决定了控制策略很难，或者不可能以云服务类型进行部署。

- √ 分析合规条例对政策和规程的影响。 将数据和应用迁移到云服务上将可能对政策和规程产生影响。消费者应该评估那些与合规条例相关的政策和规程，有关的例子包括活动报告、日志、数据保存、事故响应、控制测试以及隐私政策等。

- √ 准备满足合规需求的证据。 如何从大量的合规条例和要求中收集合规的证据将是一个挑战。云服务的消费者应该指定出收集和存储合规证据的流程，包括日志、事件报告、系统配置备份、变更管理报告和其他流程输出资料。基于云服务模型，云提供商可能需要提供类似的大量信息。

- √ 审计师的资质和选择。在很多时候组织没有权利去选择审计师或安全评估人员。如果组织有一定选择的权利（selection input），由于很多审计师对云和虚拟化技术不熟悉，强烈建议选择一个对云有一定了解的审计师。询问一下关于IaaS/PaaS/SaaS 相关术语的熟悉程度是一个不错的开始点。

- √ 云提供商的 SAS 70 Type II。提供商应该有最低级别的审计声明，因为其要为审计师和评估人员提供一个可识别的参考点。由于 SAS 70 Type II 只保证文档中安全控制的实施，所以理解 SAS 70 Type II 审计的范围和安全控制是否满足你的要求是同等重要的。

- √ 云提供商通过 ISO/IEC 27001/27002 的计划。提供关键服务的云提供商应该在信息安全管理系统中达到 ISO/IEC 27001 的标准。如果云提供商没有通过 ISO/IEC 27001 的认证，他们应该证明与 ISO 27002 实践的契合程度。

- √ ISO/IEC 27001/27002 的范围（Scoping）。云安全联盟正在业内呼吁未通过ISO/IEC 27001 认证的云提供商联合起来，以保证范围定义没有忽略关键的认证准则。

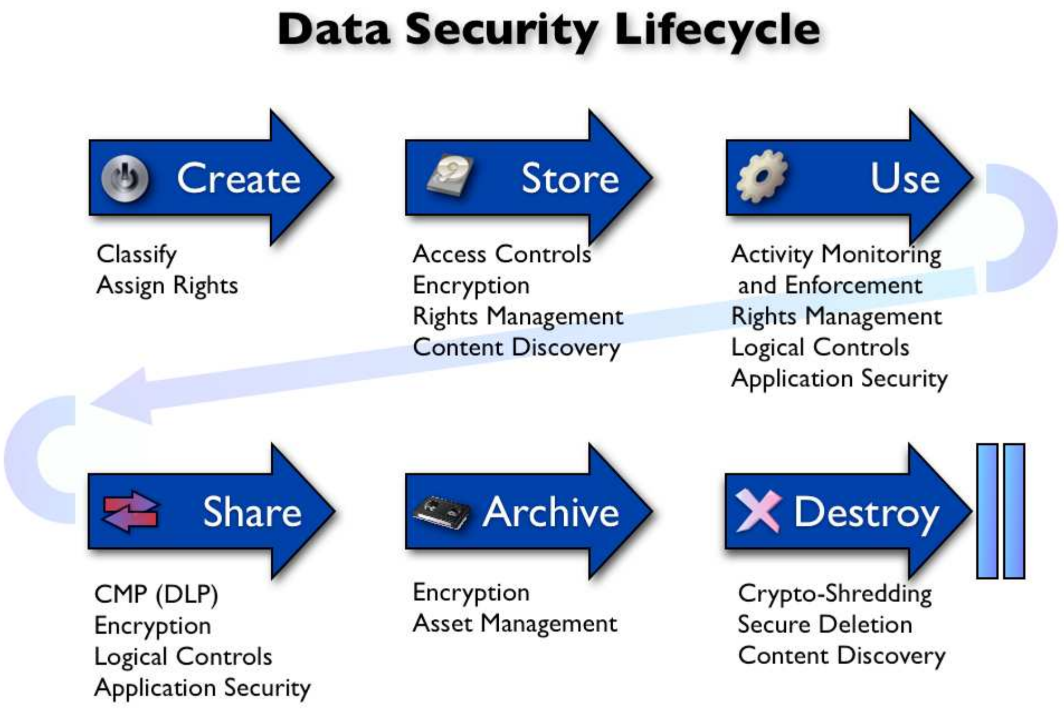
贡献者: Nadeem Bukhari, Anton Chuvakin, Peter Gregory, Jim Hietala, Greg Kane, Patrick Sullivan

D5: 信息生命周期管理

信息安全的主要目标之一是保护我们系统和应用程序的基础数据。当我们向云计算过渡的时候，传统的数据安全方法将遭到云模式架构的挑战。弹性、多租户、新的物理和逻辑架构，以及抽象的控制需要新的数据安全策略。由于许多云部署中，我们会将数据传输到外部甚至公众的环境中，这种方式在前几年是不可想象的。

信息生命周期管理

数据安全生命周期与信息生命周期管理是不同的，其反映了安全受众的不同需要。数据安全生命周期可分为六个阶段：



关于在云计算数据生命周期安全的关键挑战包括如下：

数据安全。保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

数据存放位置。必须保证所有的数据包括所有副本和备份，存储在合同、服务水平协议和法规允许的地理位置。例如，使用由欧盟的“法规遵从存储条例”管理的电子健康记录，可能对数据拥有者和云服务提供商都是一种挑战。

数据删除或持久性。 数据必须彻底有效地去除才被视为销毁。因此，必须具备一种可用的技术，能保证全面和有效地定位云计算数据、擦除/销毁数据，并保证数据已被完全消除或使其无法恢复。

不同客户数据的混合：数据尤其是保密/敏感数据不能在使用、储存或传输过程中，在没有任何补偿控制的情况下与其它客户数据混合。数据的混合将在数据安全和地缘位置等方面增加了安全的挑战。

数据备份和恢复重建（Recovery and Restoration）计划：必须保证数据可用，云数据备份和云恢复计划必须到位和有效，以防止数据丢失、意外的数据覆盖和破坏。不要随便假定云模式的数据肯定有备份并可恢复。

数据发现（discovery）：由于法律系统持续关注电子证据发现，云服务提供商和数据拥有者将需要把重点放在发现数据并确保法律和监管当局要求的所有数据可被找回。这些问题在云环境中是极难以回答的，将会需要管理、技术和必要的法律控制互相配合。

数据聚合和推理：数据在云端时，会有新增的数据汇总和推理的方面的担心，可能会导致违反敏感和机密资料的保密性。因此，在实际操作中，应要保证数据拥有者和数据的利益相关者的利益，在数据混合和汇总的时候，避免数据遭到任何哪怕是轻微的泄漏（例如，带有姓名和医疗信息的医疗数据与其它匿名数据混合，两边存在交叉对照字段）。

建议

√ 理解如何维护完整性、如何检测违反完整性、如何提交报告给客户。同样的建议适用于数据的机密性。

√ 云服务提供商必须向数据所有者保证按照 SLA 中定义的安全实践和规程提供“全面披露”（也即透明性）。

√ 确保在数据的生命周期中所使用的所有控制的都是规范和可识别的。确保所有控制对于数据拥有者和云服务提供商来说，有明确的职责分工。

√ 维持一个关于数据具体位置的基本原则。确保有能力知道存储的地理位置，并在服务水平协议 SLA 和合同中约定。在地理位置定义和强制执行方面，需要有适当的控制来保证。

√ 理解什么情况下存储可以由第三方或政府机构进行抓取。当数据拥有者的信息已经或将被抓取，需确定服务水平协议中是否规定云服务提供商要预先通知数据拥有者（如果可能）。

√ 在某些情况下，传票或取证书面命令可能会发给云服务提供商。在这种情况下，当云服务提供商具有客户数据的监护权，此提供商应告知数据所有者，他们将不得不披露数据拥有者的数据。

√ 服务惩罚的制度应包含在数据拥有者和云服务提供商之间的合同中。具体而言，合同中数据保护条款应遵从于国家和国际数据违反条例，由云服务提供商提供保护（如：加州参议院法案 1386 或新的 HIPAA 的数据违反法则）。

√ 数据的拥有者有责任来决定谁应该获得权限和特权访问数据，以及在何种条件下可以访问数据。数据的拥有者应该保持一个策略：默认状态下，所有的数据拥有者的雇员和云服务提供商没有任何访问权限。

√ 云服务提供者应通过合同化语言或合同条款，保证无权访问作为基本原则（即否认，“默认拒绝所有”）。这一原则适用于云服务提供商员工和其他顾客，而不是数据拥有者的雇员和授权访问人员。

√ 数据拥有者有责任定义和识别数据分类。云服务提供商有责任在数据拥有者制定的数据分类基础上执行数据访问控制需求，这些责任应体现在合同中，并按遵从性强化和审计。

√ 当客户被迫披露数据，必须避免“污染”数据。数据拥有者不仅必须确保所有传票，电子证据发现的裁决要求的数据是完整的，并正确披露，还必须确保没有其他数据受到影响。

√ 数据加密（参考 D11，加密和密钥管理）。

√ 确定整个 IT 架构和抽象层的信任边界。确保子系统只有在需要时才跨越安全边界，并需要配合适当的保障措施，以防止未经授权的披露、更改或销毁数据。

√ 理解云服务提供商使用了什么隔离技术来实现客户的彼此隔离。云服务提供商可能根据服务的类型和数量而使用不同隔离技术。

√ 当尝试进行数据发现时，应了解云服务提供商在数据搜索方面的能力和限制。

√ 了解多租户存储环境中是如何进行加密管理的。是所有数据拥有者共享一个密钥？每个数据拥有者各自拥有一个密钥？或者一个数据拥有者使用多个密钥？是否有制度或系统防止不同的数据拥有者使用相同的密钥？

√ 数据拥有者应要求云服务提供商确保他们的备份数据不与其他云服务的客户数据混合。

√ 理解云服务提供商存储的回收流程。在多租户环境中，数据销毁是非常困难的，云服务提供商应使用加强型加密，避免存储被任何授权以外的应用、进程和实体等非法回收、分解或读取。

√ 数据保存和销毁的计划是数据拥有者的责任。根据客户要求销毁数据是云服务提供商的责任，需要强调的是，销毁数据时候，应该包括所有位置和所有形式的数据。如有可能，数据拥有者应强制执行、并审计这些操作。

√ 了解信息的逻辑隔离和已实施的保护控制。

√ 理解自己公司委托管理的数据的固有隐私限制，数据拥有者可能需要在把数据托管给某个云服务提供商之前，先选定其作为合作伙伴。

√ 了解云服务提供商的数据保存和销毁策略和程序，并与其内部组织策略对比。请注意，云服务提供商对于数据保存的保证是较容易演示，数据销毁的演示就非常困难。

√ 需要严肃对待谈判云服务提供商发生数据外泄的相关惩罚。如果可行，客户应该要求赔偿其作为云服务提供商的合同中涉及的数据恢复的所有费用。如果不切实际，客户应探讨确定转移风险的媒介，如通过保险。

√ 定期执行备份和恢复测试，以确保逻辑隔离和控制是有效的。

√ 确保云服务提供商人员控制措施是到位的，具备合理的逻辑职责隔离 SOD。

√ 理解在多租户存储情况下如何进行加密管理。 所有客户共享一个密钥、每个客户拥有一个密钥或者每个客户拥有多个密钥？

基于 ILM 每个阶段的数据安全建议

我们会结合信息生命周期管理的每个阶段提出一些通用建议、以及其它的具体控制。请记住，建议和控制方法与云服务模式相关（SaaS、PaaS 或 IaaS），有些建议需要客户进行实施，另一些需要由云服务提供商实施。

创建

√ 识别可用的数据标签和分类。

√ 企业数字权限管理（DRM）可能是一种选择。

√ 数据的用户标记在 WEB2.0 环境中应用已经非常普遍，可能对分类数据会有较大帮助

存储

√ 识别文件系统、数据库管理系统 DBMS 和文档管理系统等环境中的访问控制。

√ 加密解决方案，涵盖如电子邮件、网络传输、数据库、文件和文件系统。

√ 在某些需要控制的环节上，内容发现工具（如 DLP 数据丢失防护）会有助于识别和审计。

使用

√ 活动监控，可以通过日志文件和基于代理的工具。

√ 应用逻辑。

√ 基于数据库管理系统解决方案的对象级控制。

共享

√ 活动监控，可以通过日志文件和基于代理的工具。

√ 应用逻辑。

√ 基于数据库管理系统解决方案的对象级控制。

√ 识别文件系统、数据库管理系统和文档管理系统等环境中的访问控制。

√ 加密解决方案，涵盖如电子邮件、网络传输、数据库、文件和文件系统。

√ 通过 DLP 实现基于内容的数据保护。

归档

√ 加密，如磁带备份和其他长期储存介质。

√ 资产管理和跟踪

销毁

√ 加密和粉碎：所有加密数据相关的关键介质的销毁。

√ 通过磁盘“擦拭”和相关技术实现安全删除。

√ 物理销毁，如物理介质消磁。

√ 通过内容发现以确认销毁过程.

贡献者: Richard Austin, Ernie Hayden, Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna Garcia, Rich Mogull, Jeff Reich

D6: 可移植性和互操作性

组织必须带着未来可能必须更换云提供商的想法走近云。可移植性和互操作性必须被作为云项目风险管理和安全保证的一部分而提前考虑。

大型的云提供商可以在云中提供提供异地灾备，这使得一个云提供商为客户提供高可用性的服务成为可能。然而，用户部署基本的业务连续性计划还是明智的，以把最坏情况造成的影响降至最低。在未来，企业可能会突然发现必须立刻更换其云提供商，主要的原因包括以下几点：

- 无法接受续约带来的费用增加
- 提供商停止了业务运营
- 提供商在没有给出合理的数据迁移计划之前，关停了企业正在使用的服务
- 无法接受服务质量的下降，比如无法完成关键业绩要求或服务级别协议（SLA）.
- 发生在云用户和提供商之间的分歧。

一些简单的架构级设计可以帮助将上述问题发生的损害降至最低。然而，解决这些问题的办法取决于云服务的类型。

使用 SaaS 的客户可以使用新软件应用替代旧的。因此，关注的重点不在于应用的可移植性，而是保持或增强旧应用程序的安全功能，以成功的完成数据迁移。

在 PaaS 情况下，为达到可移植性，一定程度上对应用的修改是需要的。关注的重点在于当保存或增加安全控制时，最大限度的降低应用重写的数量，同时成功的完成数据迁移。

在 IaaS 情况下，关注的重点和期望是应用和数据都能够迁移到新的云提供商并顺利运行。

由于缺乏可操作性方面的标准，也缺乏对此类标准的市场压力，在云提供商之间的转换可能会是一个痛苦的手工过程。从安全的角度看，我们主要的关注点（concerns）是在环境变更时维护安全控制的一致性。

<u>建议</u>

针对所有的云解决方案:

√ 更换云提供商，至少对于一方来说，实际上是一种消极的商业业务，可能会导致来自于上一家云提供商的无法预计的消极反应。这必须在合同过程中（D3）、业务连续性规划（D7）和全局治理（D2）中加以计划。

√ 理解托管在云提供商处的数据集合的规模。数据规模的偏差可能导致在传输中的服务中断，或者是超出预期的传输周期。很多用户发现在传输大量数据时，使用人工快递硬盘比电子传输的速度要快。

√ 用文档记录安全架构和每一个安全组件的配置，这些文档可以用以内部审计，同时也有利于未来向新提供商的迁移。

针对 IaaS 云解决方案:

√ 理解新的云提供商是如何采集和移植虚拟机镜像的，因为其可能使用不同的虚拟化技术。

√ 识别和去除（至少记录）虚拟机环境中特殊的提供商扩展。

√ 理解在应用已经完成从云提供商的移植后，是否有措施到位来保证恰当地删除（decommission）虚拟机镜像。

√ 理解硬盘和存储设备“退役”的实践做法。

√ 理解以硬件/平台为基础的依赖关系，并在应用/数据迁移之前识别出来。

√ 向之前的云提供商索取系统日志、线索（traces）的访问权限，以及访问和账单记录。

√ 如果新提供商的服务质量不能令人满意，选择与前云提供商重新开始或延续一部分或整体服务。

√ 确定现有系统中是否存在任何与新提供商不兼容的、或者是新提供商尚未实现的管理功能、接口或者应用程序接口（API）。

针对 PaaS 云解决方案:

√ 尽可能的使用那些采用标准语法、开放应用程序接口和开放标准的平台组件。

√ 理解哪些工具可以用来做安全的数据传输、备份和恢复。

√ 理解并文档记录 PaaS 提供商特殊的应用组件和模块，并开发包含抽象层次的应用架构以减少对私有模块的直接访问。

√ 理解类似监控、日志记录和审计等基础服务在新提供商的系统中如何传送。

√ 理解前云提供商提供的控制功能，以及如何将其过渡到新提供商的系统中。

√ 当迁移到一个新平台时，理解其对应用的性能和可用性的影响，以及这些影响的衡量办法。

√ 理解如何在迁移之前和之后完成测试，以确保服务和应用运行正常。保证提供商和客户都清楚自己的测试责任并进行文档记录。

针对 SaaS 云解决方案:

√ 执行常规的数据提取和备份，以保证其在非 SaaS 模式下可用。

√ 理解元数据是否可以被保存和迁移。

√ 理解现有系统中是否存在任何定制工具，在将来需要被重新开发或者新的提供商必须提供这些工具。

√ 保证在不同云提供商之间控制的一致性。

√ 保证以下数据或文件的可移植性，包括备份和日志、访问记录的其余拷贝，以及其他任何可能因法律和合规原因被要求的信息。

√ 理解管理、监控和报表接口，及其在不同环境之间的整合方式。

√ 对于新的提供商，是否有条款规定在移植前去测试和评估应用程序？

贡献者: Warren Axelrod, Aradhna Chetal, Arthur Hedge, Dennis Hurst, Sam Johnston, Scott Morrison, Adam Munter, Michael Sutton, Joe Wallace

第三部分：云的运行

D7: 传统安全、业务连续性和灾难恢复

传统的物理安全、业务连续性计划（BCP）和灾难恢复（DR）等形成的专业知识与云计算仍然有紧密关系。由于云计算的迅速变化和缺乏透明度，这就要求在传统的安全、业务连续性规划和灾难恢复领域的专业人员不断进行审查和监测您所选择的云服务供应商。

当前我们面临的的挑战是如何合作进行风险识别、确认相互依存、整合、动态并且有效的利用资源。云计算和与之配套的基础设施可以帮助减少某些安全问题，但也可能会增加某些安全问题，肯定不会消除人们对安全的需要。随着业务和技术领域的重要变革的深入，传统安全原则依然存在。

建议

√ 必须谨记，数据的集中意味着云服务提供商内部人员的“滥用”是一个重大的问题。

√ 云服务提供商应考虑采纳大多数客户的最严格的需求作为一个安全基准。在一定程度上，这些安全实践不会对客户的体验产生负面影响；从长远来说，在降低风险以及客户驱动的安全领域的关注方面，严格的安全实践应当可以被证明有很好的成本效率。

√ 云服务提供商应对工作职责建立强健的隔离制度，并且对要对员工进行背景调查，要求/强制执行的非雇员的保密协议的签订，并且按照“履行职责的绝对需要”来限定员工对客户知识的了解。

√ 客户应尽可能对云服务提供商的设施进行现场检查。

√ 客户应该检查云服务提供商灾难恢复和业务连续性计划。

√ 客户应辨识提供商基础设施的实际物理的相互依存关系。

√ 确保在合同中，对安全、恢复以及数据访问有一个权威的分类明确地阐明有关安全、恢复、以及对数据的访问。

√ 客户应该要求提供者的内部和外部的安全控制文件，并遵守某些行业标准。

√ 确保恢复时间目标（RTO）已经被客户充分理解并且已经订立契约关系，并且已经在纳入技术规划过程。确保技术路线图、政策和运作能力能够满足这些要求。

√ 客户需要确认提供商提供的现有的 BCP 政策已经被提供商的董事会批准。

√ 客户应寻求管理层的积极支持，并定期审查业务连续性程序，以确保业务连续性程序是“活”的。

√ 客户应检查 BCP 是否被认证和/或被诸如 BS 25999 之类国际公认标准认定。

- √ 客户应该确定提供商是否有任何在线资源致力安全和 BCP，且该计划的概要和清单可以供人们参考。

- √ 确保云服务提供商已经通过该公司销售商安全过程（VSP）的审核，以便对共享了哪些数据以及采用了什么样的控制手段有一个清楚地了解。VSP 决定应该将风险是否可以接受反馈给给决策过程和决策评估。

- √ 由于云计算的动态和相对“年轻”的特性，上述所有活动需要更加频繁的周期来披露还没有和消费者沟通的变化。

贡献者: Randolph Barr, Luis Morales, Jeff Spivey, David Tyson

Copyright © 2010 Cloud Security Alliance

D8: 数据中心运行

当业务和客户的 IT 服务转移到云计算的时候，云服务提供商的数量在不断地增长。为了给不断增长的云计算服务提供燃料，相应的数据中心数量也出现了同样的增长。所有类型和规模的云服务提供商，包括知名的技术领导者或数以千计的起步者或新兴成长型公司，都在这一充满希望的新 IT 服务交付形式上投入巨资。

通过 IT 资源共享来创造效率和规模效益并不是一个新概念。如果对数据中心的运营进行传统的庞大的投资能带来更多的客户，那么云的商业模式效果最好。传统的数据中心架构设计上会特意超出周期性的负载高峰，也就是说在正常或闲时，数据中心的资源往往闲置很长一段时间而不被充分利用。相反，云服务提供商为了赢得竞争优势最大限度地提高运营利润率，他们通过人力和技术手段寻求资源的优化使用。

云服务的消费者面临的挑战是如何最好地评估云服务提供商是否有能力提供正确的和有成本效益的服务，同时又能保护客户自己的数据和利益。不要假设云服务提供商会将消费者最感兴趣的东西作为他们的最高优先级。由于云计算作为一种基本的“运营商”的服务交付形式出现，因而当超出合同管理水平的时候，云计算服务提供商通常有很少或者不允许访问或者控制客户的数据和系统。当然，这种做法是正确地。但有些云计算架构可能对客户的数据完整性和安全性采取相对“自由”（liberties）的做法，如果客户意识到这些做法可能会感到不舒服。通过询问适当的问题、并且熟悉基础架构和可能出现安全漏洞的地方，客户自己针对自己计划中的云服务开展教育。

在作出决定要将所有或部分业务转移到云时，首先要了解云服务提供商如何实现 D1 中所论述的“云计算的 5 大关键特征”的，其次它的技术架构和基础设施是否会影响满足服务水平协议 SLA 和解决安全问题的能力。云服务提供商可能将 IT 产品和其它云服务的组合作为自己的某个具体技术的基础架构，例如利用了其它云服务提供商的 IaaS 存储服务。

不同云服务提供商的在技术架构和基础设施可能会有所不同，但是为了符合安全要求，他们都必须全部能够展示系统、数据、网络、管理、部署和人员方面的全方位相互隔离。为了不互相干扰，每一层基础设施的控制隔离需要适当加以整合。例如，检查存储划分是否可以很容易地通过管理工具或不好的密钥管理绕过。

最后，了解云服务供应商如何处理资源动态分配，以便在商业系统的正常起伏波动过程中预测系统可用性和性能的适当水平。请记住，云计算理论还超前于它的实践：许多客户对所涉及的自动化水平作出了不正确的假设。在配置资源达到容限时，云服务提供商要确保其它的资源可以及时地无缝地提供给客户。

建议

假设有一个组织考虑购买云服务，无论是什么样的云服务，他必须很明确的知道合同中哪些服务是包括的，哪些服务是不包括的。以下总结的信息需要时刻审视，包括：云服务提供商的选择流程，选择服务提供商资质以更好匹配服务与组织需求的一些额外的问题等。

- √ 无论云服务提供商拥有哪种资质，重要的是获得承诺或授权进行客户方或外部第三方审计的权利。

√ 云客户应了解云服务提供商如何实现 D1 中阐述的“云计算的五大关键特征”，以及技术架构和基础设施如何影响他们满足服务水平协议 SLA 的能力。

√ 不同云服务提供商的在技术架构和基础设施可能会有所不同，但是为了符合安全要求，他们都必须全部能够展示系统、数据、网络、管理、部署和人员方面的全方位相互“隔离”。

√ 了解你的云服务提供商如何在你业务发生波动时调动资源以提供最佳的系统可用性和性能。如果可行的话，找一找云服务提供商的其它客户，评估一下他们的业务波动时可能会对您的云服务提供商的客户体验影响。一定要确保服务水平协议 SLA 被清晰定义、可衡量、可强制执行、并且如你所需得到充分满足，没有什么可以替代。

√ 客户应该清楚自己的云服务提供商的的补丁管理政策和程序以及这些可能对他们系统环境的影响。这种理解应反映在合同中。

√ 由于针对某个客户进行的任何政策、流程、程序、或工具的改进都可能会导致所有客户服务的改善，所以在云服务环境中持续改进显得尤为重要。寻找那些具备标准的持续改进流程的云服务提供商。

√ 技术支持或服务台通常是一个云服务提供商面向客户的业务窗口。为了给你的最终用户带来一个平稳、统一的客户支持经验，必须确保云服务提供商的客户支持流程、程序、工具以及支持时间与你的兼容。

√ 正如 D7 讲的那样，用 IT 视角去审视业务连续性和灾难恢复计划，看看他们如何与人力和流程关联的。例如，云服务提供商的技术架构可能会在故障切换上采用了新的、未经验证的方法。客户自己的业务连续性计划也应解决云计算的影响和局限性。

贡献者: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Alexander Windel, Richard Zhao

D9: 应急响应、通告和补救

由于云计算的本质，所以当发生安全事件、数据破坏、或其他需要调查和采取行动该找谁时显得更难以确定。为了满足相同汇报责任的需求的变化，需要修改标准安全事件响应机制。本章节提供了如何处理这些事件的指导。

对于客户来说，部署到云的应用程序并不总是把数据完整性和安全性设计放在第一位的。这可能导致脆弱的应用部署进云环境，进而引发安全事故。此外，基础设施架构的缺陷、加固规程中的错误、以及简单的操作疏忽都会对云服务的运营构成重大的威胁。当然，类似的漏洞同样也会危及传统的数据中心的运营。

很明显，事件处理过程需要专业技术知识，但隐私和法律专家对云安全同样可以作出重大贡献。在事件响应中，他们还会在通知、补救、以及随后可能采取的法律行动中发挥关键作用。如果一个组织考虑使用云服务，那么他需要审视有关未被用户协议和隐私政策制约的员工对数据的访问的机制是否已经实施。在 IaaS 和 PaaS 架构中，云服务提供商自己的应用程序不管理应用程序数据，这和 SaaS 提供商的应用程序控制数据有所不同。

大型云服务提供商交付 SaaS、PaaS 和 IaaS 服务的复杂性造成重大事件响应过程中的隐患，潜在客户必须评估相应 SLA 的可接受水平。在评估云服务提供商时，很重要的一点事要意识到供应商可能托管了成百上千的应用程序实例。从事件监测的角度讲，任何外部应用程序都会拓宽安全运行中心（SOC）的责任。通常，SOC 监测那些由入侵检测系统和防火墙中产生预警和其他事件的指标，但是，在开放的云环境中这些必须监测的消息来源和通告的数量将会以指数方式增长，例如，SOC 可能需要监测消费者之间的活动，还有外部事件。

一个组织需要了解他们所选择的云服务提供商的事件响应策略。这一策略必须解决识别和通知，以及针对应用程序数据的未经授权访问的补救选项。更为复杂的是，在不同的数据存放位置，应用数据的管理和访问有不同的含义和监管要求。例如，如果涉及到的数据在德国，有事件发生，可是如何数据在美国，可能就不认为是“事件”。这使得事件识别充满挑战性.

建议

√ 在服务部署前，云客户要明确界定，并且和云服务提供商沟通什么是他们认为的事故（incident）（如数据破坏），什么仅仅是事件（event）。

√ 云客户参与云服务提供商的事件响应活动可能非常有限。因此，客户了解与云服务提供商的事件响应小组的既定沟通路径非常关键。

√ 云客户应该调查云服务提供商使用哪些事件检测和分析工具，以确保他们对自己的系统兼容。在联合调查，特别是那些涉及法律调查（discovery）或政府干预（intervention）时，云服务提供商的某个私有的或者非常规格式的日志往往会成为主要障碍。

√ 设计和保护不当的应用程序和系统可以很容易地“淹没”每个人的事件响应能力。对系统进行适当的风险管理，并且利用纵深防御的做法在第一时间减少发生安全事件的机会是很关键的。

√ 安全运行中心（SOC）经常假定对事件响应上只有一个单一的管控模型，但是这对多租户的云服务提供商来说并不恰当。一个强劲而良好维护的安全信息和事件管理（SIEM）流程用以识别可用数据源（应用程序日志、防火墙日志、以及 IDS 日志等等），并且将这些日志合并进可以协助 SOC 检测云计算环境事件的通用分析告警平台。

√ 为了极大地方便的进行详尽的离线分析，可以考察能够提供整个客户虚拟环境快照的能力的云服务提供商，这些快照包括防火墙、网络（交换机）、系统应用程序和数据。

√ 遏制（containment）是破坏控制和搜集证据之间的一场赛跑。基于机密性－完整性－可用性（CIA）这样三位一体的遏制做法才是有效的。

√ 补救突出了能够将系统恢复到某个先前状态的重要性，甚至需要回到 6 个月或 12 个月前的已知可用配置。将法律选择和要求牢记在心，补救可能还需要支持事件数据的“事后分析”（forensics）记录。

√ 所有因为数据泄漏监管而被分类为“私有”的数据都应该加密，以减少泄漏事件带来的后果。客户应在合同中规定相关的加密要求，具体参见 D11。

√ 有些云服务提供商可能拥有一大批拥有独特应用的客户。为了能够给每一个特定客户提供细颗粒度的事件，这些云服务提供商应该考虑应用层日志框架。这些云服务提供商还应该构建一个注册表，按照应用程序接口（URL、SOA 服务、等）来记录应用程序所有者。

√ 在多租户环境下，应用级防火墙、代理服务器，以及其它的应用日志工具是当前可用的协助事件响应的关键能力。

贡献者: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Alexander Windel, Richard Zhao

D10: 应用安全

由于云环境其灵活性、开放性、以及公众可用性这些特性，给应用安全的基本假设带来了很多挑战。这些假设中的一部分可以很好理解，而很多却不容易理解。从设计到运维再到最终退役，本章节试图阐述云计算如何对一个应用程序的生命周期安全产生影响。本指南对所有参与者有关，包括应用程序的设计人员、安全专业人员、运维人员以及技术管理者等，阐述如何最好地降低云计算应用程序的风险并管理其保障措施。

在所有 SaaS、PaaS、IaaS 的所有层面，对于应用程序来说，云计算都是一个特别的挑战。基于云计算的应用软件需要经过类似于 DMZ 区部署的应用程序那样的严格设计。这包括了深入的前期分析，涵盖了传统的如何管理信息的机密性、完整性，以及可用性等方面。

在云环境下，应用程序将会对以下重大方面产生影响或被影响：

- **应用安全架构** – 必须意识到这样一个事实，大多数应用程序会与其它多个不同的系统产生依赖关系。有了云计算，应用程序的依赖性可能非常动态，甚至每个依赖都代表一个独立的第三方服务提供商。云特性使配置管理和紧随的配置供应比传统的应用程序部署更为复杂。为了保证应用程序的安全，云环境推动了应用程序架构的变革。

- **软件开发生命周期（SDLC）** – 云计算影响 SDLC 的各个方面，涵盖应用程序体系结构、设计、开发、质量保证、文档、部署、管理、维护和退役。

- **合规性** – 合规性明显会影响数据，而且也会影响应用程序（例如，监管要求如何实现程序中的一个特定加密函数）、平台（对操作系统的控制和设置的命令）和进程（如对安全事件的报告要求）。

- **工具和服务** – 围绕着开发和维护运行应用程序需要的工具和服务，云计算对工具和服务带来了一系列的新挑战。这其中包括开发和测试工具、应用程序管理工具、对外服务的耦合、以及库和操作系统服务的依赖性，这些可能都源自云服务提供商。了解谁提供、谁拥有、谁运行的后果、并承担相关的责任非常重要。

- **脆弱性** – 这不仅包括很好文档化的和不停演化中的 web 应用脆弱性，还有那些在机器与机器之间的、面向服务架构（SOA）的应用程序的脆弱性，这些 SOA 应用正在不断地被部署进云中。

<u>建议</u>

√ 软件开发生命周期（SDLC）的安全很重要，应该在高层次上解决基于云开发的三个主要的差异化：1）更新的威胁和信任模型；2）更新的、云环境下的应用评估工具；3）能够说明云应用安全体系架构变化的 SDLC 的过程和质量检查点。

√ IaaS、PaaS 和 SaaS 为软件开发生命周期创造了不同的信任边界，这些都必须在应用的开发、测试以及生产部署过程中得到证明。

√ 对于 IaaS，成功的关键因素是是否存在可信的虚拟机镜像（image）。最好的办法是能够提供符合你内部政策的虚拟机镜像。

√ 虚拟机应该使用 DMZ 主机系统的加固方案的最佳实践。只开放支持应用“堆栈”所需的服务。

√ 保护主机之间的通信安全是基本原则。不要做主机之间存在安全通道的假设，不管是在常用的数据中心或者在同一台硬件设备上。

√ 管理并且保护的应用的证书和密钥至关重要。

√ 应加倍小心的处理应用程序的日志和调试记录的文件，因为这些文件的位置可能偏远或不明，而且上面的信息可能很敏感。

√ 在应用威胁模型中考虑外部管理和多租户场景。

√ 对于比较复杂的应用程序，可能会采用企业服务总线（ESB），需要使用某个协议直接保护 ESB，例如 WS-Security 协议。在 PaaS 环境下不具备隔离 ESB 的能力。

√ 应采用度量方式评估应用程序安全计划的有效性。在直接的具体到应用的安全指标中，可用的包括漏洞分数和补丁覆盖范围等。这些指标会显示应用程序代码的质量。间接的数据处理指标，像加密数据的百分比，会从应用程序架构的角度指出是否在作出负责任的决定。

√ 云服务提供商必须支持对他们云环境的应用程序进行 WEB 动态安全分析工具的使用。

√ 应留心恶意行为者在出现一个新的云应用架构，能在监视下掩盖某些应用组件时会如何反应。黑客喜欢攻击能看到代码，包括但不限于在用户环境中运行的代码。他们很可能会攻击基础设施，并进行大面积的黑盒测试。

√ 客户应该获得合同中规定的权限来执行远程漏洞评估，包括传统的（网络/主机）和应用程序漏洞评估。由于供应商的无法区分测试和实际攻击，也为了避免对其他客户产生潜在影响，许多云服务提供商限制漏洞评估。

贡献者: John Arnold, Warren Axelrod, Aradhna Chetal, Justin Foster, Arthur J. Hedge III, Georg Hess, Dennis Hurst, Jesus Luna Garcia, Scott Matsumoto, Alexander Meisel, Anish Mohammed, Scott Morrison, Joe Stein, Michael Sutton, James Tiller, Joe Wallace, Colin Watson

D11: 加密和密钥管理

云用户和提供商需要避免数据丢失和被窃。如今，个人和企业数据加密都是强烈推荐的，甚至有些情况下是世界范围法律法规强制要求的。云用户希望他们的提供商为其加密数据，以确保无论数据物理上存储在哪里都受到保护。同样的，云提供商也需要保护其用户的敏感数据。

强加密及密钥管理是云计算系统需要用以保护数据的一种核心机制。由于加密本身不能保证防止数据丢失，因此法律法规中的责任避风港（safe harbor provisions）将加密数据的丢失看作根本没有丢失。加密提供了资源保护功能，同时密钥管理则提供了对受保护资源的访问控制。

加密的机密性和完整性

云环境由多个“租户”共享，服务提供商对于这个环境中的数据有特许存取权。因此云中存储的机密数据必须通过访问控制组合（见 D12）、合同责任（见 D2、D3、D4）和加密措施（本章描述）等进行保护。其中，加密提供的好处有：对云服务提供商的依赖性最小、减少对运行错误（operational failures）检测的依赖性。

加密网络传输中的数据。加密在网络中传输的多用途机密数据（credentials）是极其必要的，比如信用卡号、密码和私钥等。虽然云提供商网络可能比开放网络安全，但是他们使用其特有的、由许多不同的组成部分构成的架构，且由不同的组织共享云。因此，即便是在云提供商的网络中，保护这些传输中的敏感数据和受监管信息也是非常重要的。通常情况下，这些在 SaaS、PaaS 和 IaaS 环境中实施起来的难易程度是一样的。

加密静止数据。加密磁盘上的数据或生产数据库中数据很重要，因为这可以用来防止恶意的云服务提供商、恶意的邻居“租户”及某些类型应用的滥用。对于长期的档案存储来说，一些用户加密他们自己的数据然后发送密文到云数据存储商。这些客户控制并保存密钥，在自己需要的情况下解密数据。在 IaaS 环境中，使用多种提供商和第三方工具加密静止数据很普遍。在 PaaS 环境中加密静止数据一般会较复杂，需要提供商提供的或专门定制的设备。在 SaaS 环境中加密静止数据是云用户无法直接实施的，需要向他们的提供商请求。

加密备份媒介中的数据。这可以防止对丢失或被窃媒介的滥用。理想的情况是云服务提供商以透明模式实施。但是，作为用户和数据提供者，验证是否有这种加密是你自己的责任。对加密基础设施的一个考虑因素是处理数据的寿命。

除这些常见的加密应用之外，对云提供商可能遭受的特殊攻击同样要求进一步分析加密动态数据的方式，包括内存中的数据。

密钥管理

现有的云服务提供商可以提供基础加密密钥方案来保护基于云的应用开发和服务，或者他们将这些保护措施都交由他们的用户决定。当云服务提供商向支持健壮密钥管理的方案发展时，需要做更多工作来克服采用的障碍。正在制定的标准应该在不久的未来解决这个问题，但是工作仍然在进行中。云计算中还有很多密钥管理有关的问题和挑战。

保护密钥存储（Key Store）。密钥存储必须像其他敏感数据一样进行保护。在存储、传输和备份中都必须保护。不适当的密钥存储可能危害所有加密数据。

访问密钥存储。必须限制只有特定需要单独密钥的实体可以访问密钥存储。还需要相关策略来管理密钥存储，使用角色分离来帮助进行访问控制：给定密钥的使用实体不能是存储该密钥的实体。

密钥备份和恢复。丢失密钥无疑意味着丢失了这些密钥所保护的数据。尽管这是一种销毁数据的有效过程，但是意外丢失保护关键任务数据的密钥会毁灭一个业务，所以必须执行安全备份和恢复解决方案。

有很多标准和指导方针适用于云中的密钥管理。OASIS 密钥管理协同协议（KMIP）就是云中协同密钥管理的新标准。IEEE1619.3 标准涵盖了存储加密和密钥管理，尤其适用于存储 IaaS。

建议

√ 使用加密把数据使用与数据保管分离。

√ 把存放数据的云服务提供商与密钥管理分开，建立一系列的“分离”（separation）。这即保护了云提供商，也保护了用户。避免其由于法律要求而提供数据时产生冲突。

√ 当在合同中约定加密时，确保加密遵循了相关行业和政府标准。

√ 了解是否云提供商的设施提供了角色管理及职责分离。

√ 如果云提供商必须进行密钥管理，了解提供商是否定义了密钥管理生命周期的过程：密钥如何产生、使用、存储、备份、恢复、轮换和删除。而且，了解是否每个客户使用了相同密钥或是否每个客户有其自己的密钥系列。

√ 除了确保受监管和/或敏感客户数据在静止时是加密的之外，还要确保在其在云提供商的内部网络传输时是加密的。在 IaaS 环境中，这将由云用户选择实施；在 PaaS 环境中，由用户和提供商共同分担责任；在 SaaS 环境中，由云提供商来负责。

√ 在 IaaS 环境中，理解由传统加密分别保护的敏感信息和关键材料如何在使用中可能暴露（exposed）。例如，虚拟机交换文件与其他临时数据存储位置可能也需要进行加密。

贡献者: John Arnold, Girish Bhat, Jon Callas, Sergio Loureiro, Jean Pawluk, Michael Reiter, Joel Weise

D12: 身份和访问管理

管理身份和访问企业应用程序的控制仍然是当今的 IT 面临的最大挑战之一。虽然企业可以在没有良好的身份和访问管理策略的前提下利用若干云计算服务，从长远来说延伸企业身份管理服务到云计算确是实现按需计算服务战略的先导。因此对企业基于云的身份和访问管理（IAM）是否准备就绪进行一个诚实的评估，以及理解云计算供应商的能力，是采纳现今公认为不成熟的云生态系统的必要前提。

我们将讨论以下几个在云中实施成功有效的身份管理必不可少的 IAM 功能：

- 身份供应/取消供应（provisioning/deprovisioning）
- 认证
- 联盟
- 授权和用户配置文件管理

合规是整个过程的关键考虑因素。

身份供应：对企业采纳云计算服务机构的主要挑战之一是在云端安全和及时地管理报到（供应，即创建和更新帐户）和离职（取消供应，即删除用户帐户）的用户。此外，已经实行内部用户管理的企业将寻求将这些进程和实践引伸到云端服务。

认证：当机构开始利用云端服务时，以可信赖及易于管理方式来认证用户是一个至关重要的要求。机构必须解决跟身份认证有关的挑战，例如凭证管理、强认证（通常定义为多因素身份认证）、委派身份认证、及跨越所有云服务类型的信任管理。

联盟：在云计算环境，联盟身份管理在使企业能够利用所选择的身份提供商（IdP）去认证云用户提供了至关重要的作用的。在这方面，身份提供商（IdP）与服务提供商（SP）以安全的方式交换身份属性也是一个重要的要求。机构在考虑云联盟身份管理应该了解的以下各种挑战和可能的解决方案，这包括有关身份生命周期管理、可用的认证方法来保护机密性和完整性；与此同时支持不可抵赖性。

授权和用户配置文件管理：为用户配置文件和访问控制方针的要求， 取决于用户是否以自己的名义行事（如消费者）或作为一个机构（如雇主，大学，医院的成员，或其他企业）。在 SPI 环境下的访问控制的要求包括建立可信任用户配置文件和规则信息，不但用它来控制在云端服务的访问，而且运行方式符合审核的要求。

<u>身份供应 - 建议</u>

√ 由云供应商提供的身份供应功能目前没有足以满足企业的需求。客户应避免专用的解决方案诸如创建云供应商独有的自定义连接器，因为这些加剧了管理的复杂性。

√ 客户应利用由云供应商提供标准的连接器，这些最好是建立在服务供应标记语言 SPML 模式上。若您的云供应商目前尚未提供，您应该要求 SPML 支持。

√ 云客户应修改或扩展其权威身份数据库（authoritative repositories），以便它包括在云端的应用和进程。

<u>认证 - 建议</u>

云提供商和客户企业都应考虑与凭证管理和强认证相关的挑战，并实施符合成本效益的解决方案来适当地减少风险。

SaaS 和 PaaS 提供商通常提供的选择是内置的认证服务到他们的应用程序或平台，或将认证以委派身份（delegating authentication）方式呈交给企业。

客户有以下几种选择：

√ 企业认证。企业应考虑通过他们的身份认证提供者（IdP）的认证用户，并通过联盟方式建立与 SaaS 提供商的信任。

√ 个人用户以自己的名义认证。企业应该考虑使用以用户为中心的认证方式，如谷歌、雅虎、OpenID、及 Live ID 等，建立能在多个网站有效使用的单套凭据（credentials）。

√ 任何 SaaS 提供商如果需要依赖专有方法来委托认证（例如，用共享加密的 cookie 或其他方式来处理可信性），在此情况下应做一个彻底适当的安全评价后，方可继续。通常应优先采纳使用开放标准的委托认证方法。

对于 IaaS，认证方面可以利用现有企业的能力。

√ 对于 IT 人员，建立一个专门的虚拟专用网（VPN）将是一个更好的选择，因为他们可以利用现有的系统和过程。

√ 一些可能的解决方案包括建立一个通往公司网络或联盟的专门 VPN 隧道。当应用程序利用现有的身份管理系统（如 SSO 方案管理系统或基于 LDAP 身份认证提供的权威身份数据源）时，专门 VPN 隧道技术可发挥更好功用。

√ 在专用 VPN 隧道是不可行的情况下，应用程序的设计应该接受各种形式的身份认证断言（SAML、WS-Federation 等），结合如 SSL 标准的网络加密技术。这种方法能使机构不仅在企业内部配置联合 SSO 的，而且可应用到云端应用程序。

√ OpenID 是当应用程序是针对企业用户之外使用的另一个选择。然而，由于 OpenID 的凭据控制是在企业外部， 因此应适当限制这些用户的访问权限。

√ 任何云提供商实施的本地认证服务应兼容开放式认证-OATH。OATH 兼容的解决方案将可避免公司被锁定成为只能够接受某一个供应商的身份认证凭据。

√ 为了能应用强认证（不论是哪种技术）， 云应用程序都应该支持委托认证给享用此程序的企业 ，例如通过 SAML 的服务。

√ 云供应商应该考虑支持各种强认证选择，例如一次性密码、生物识别、数字证书和 Kerberos。这将为企业使用他们现有的基础设施提供另一种选择。

<u>联盟 – 建议</u>

在云计算环境，身份联盟是可使联盟的企业进行身份认证、提供单一或减少登录系统（SSO）、服务提供商（SP）和身份提供者（IdP）之间的交换身份属性等的关键。机构在考虑云联合身份管理应该了解的各种挑战和可能的解决方案，以解决有关身份生命周期管理、身份认证方法、令牌格式、和不可抵赖性。

√ 企业在寻找云提供商过程中应确认云提供商支持至少有一个突出的标准（SAML 和 WS - Federation）。 SAML 是正在成为一个得到广泛支持的联盟标准，主要的 SaaS 和 PaaS 云提供商都支持。支持多标准能实现更大程度的灵活性。

√ 云提供商应该有更灵活地接受来自不同的身份提供者的标准联盟格式。但大部分云供应商当前只支持单一的标准，例如，SAML 的 1.1 或 SAML 2.0。渴望支持多种格式联盟令牌（Token）的云提供商商应该考虑采取某些类型的联盟网关（federation gateway）。

√ 机构可能希望评估比较联盟公共 SSO 与联盟私有 SSO。联盟公共 SSO 的是基于标准， 例如 SAML 和与云供应商的 WS-Federation，而联盟私有 SSO 则在 VPN 上利用现有的 SSO 架构。长远而言，联盟公开 SSO 将是最理想的，但如果机构有一个成熟的 SSO 架构，并且云部署数量有限的话，可能会从联盟私有 SSO 获得短期的成本效益。

√ 机构不妨选择联盟网关来外部化（externalize）联盟实施，以便管理令牌的签发和核查。 使用这种方法，机构委托联盟网关签发不同类型的令牌，并且联盟网关还处理把令牌从一种格式转换到另一个格式。

<u>访问控制 – 建议</u>

选择或审查云服务访问控制解决方案是否足够，需要以下考虑许多方面：

√ 审查访问控制模型的服务或数据类型是否适当。

√ 识别策略和用户配置信息的权威来源。

√ 评估所需的数据隐私策略的支持。

√ 选择一种格式， 用以规定策略和用户信息。

√ 确定从策略管理点（PAP）到策略决策点（PDP）的策略传输机制。

√ 确定从策略信息点（PIP）到策略决策点（PDP）的用户信息传输机制。

√ 从策略决策点（PDP）请求一个策略决定。

√ 在策略执行点（PEP）强化一个策略执行。

√ 计录审计所需的日志资料。

身份作为服务 IDaaS – 建议

身份作为服务（IDaaS）应遵循与内部的 IAM 部署同样的最佳实践，都辅以保密性、完整性、和可审计性的考虑。

√ 对于内部企业用户，保管人必须审查云供应商的选择以提供到云端的安全访问，或者直接通过 VPN，或者通过诸如 SAML 和强认证等行业标准。需要平衡使用云的成本降低与所需的风险缓解措施，应该解决掉将雇员信息存储在外部天然会带来隐私的担忧。

√ 对于诸如伙伴的外部用户，信息所有者需要与 IAM 的提供商在 SDLC 生命周期上合作，并将威胁评估也考虑进来。应用安全 – 各个组件之间的相互作用、以及由此产生的脆弱性（如 SQL 注入和跨站脚本，等等） - 也必须考虑和保护。

√ PaaS 用户应研究 IDaaS 提供商对行业标准支持程度，包括供应、认证、对访问控制策略的通信、以及审计信息。

√ 专有的解决方案对云端的 IAM 环境构成重大风险，这是因为专有组件缺乏透明度。专有网络协议、加密算法和数据通信往往不太安全、不太可靠、，互操作性不够等。所以对外部化的 IAM 组件采用开放标准非常重要。

√ 对于 IaaS 客户，用于发布虚拟服务器的第三方系统镜像（images），需要验证用户和镜像的真实性。对镜像的生命周期管理提供支持的审查必须与验证内部网络上安装的软件遵循同样的原则。

贡献者: Subra Kumaraswamy, Sitaraman Lakshminarayanan, Michael Reiter, Joseph Stein, Yvonne Wilson

D13: 虚拟化

利用虚拟化带来的经济上的可扩展有利于加强在基础设施、平台、软件层面提供多租户云服务的能力，然而利用这些虚拟化技术也会带来其它安全问题，本域将考虑这些安全问题。虚似化技术有许多种，最常用的是操作系统虚拟化，本版本的指南将主要针对这一技术，如果云服务的基础设施采用了虚拟机（VM）技术，这些 VM 系统间的隔离加固是必须要考虑的。

虚拟操作系统管理方面的实践现状是：大多数提供缺省安全保护的进程都未被加入，因此必须特别注意如何代替它们的功能。虚拟化技术本身引入了 hypervisor 和其它管理模块这些新的攻击层面，但更重要的是虚拟化对网络安全带来的严重威胁，虚拟机间通过硬件的背板而不是网络进行通信，因此，这些通信流量对标准的网络安全控制来说是不可见的，无法对它们进行监测、在线封堵，类似这些安全控制功能在虚拟化环境中都需要采用新的形式。

数据混合在集中的服务和存储中是另一需考虑的问题，云计算服务提供的集中数据在理论上应比在大量各种端点上分布的数据更安全，然而这同时也将风险集中了，增加了一次入侵可能带来的后果。

还有一个问题是不同敏感度和安全要求的 VM 如何共存。在云计算中，某一最低安全保护的租户，其安全性会成为多租户虚拟环境中所有租户共有的安全性，除非设计一种新的安全结构，安全保护之间不会通过网络相互依赖。

建议

√ 如果你的云提供商提供了虚拟化，识别清楚提供的是哪一种虚拟化。

√ 应通过第三方安全技术提供分层安全控制，减少对平台提供商的依赖性，加固虚拟操作系统。

√ 设法搞清 VM 内部采用了哪些安全控制，除了内置的 hypervisor 隔离——如入侵检测、反病毒、脆弱性扫描等，缺省配置达到的安全等级必须达到或超过业界基本的安全要求。

√ 搞清 VM 外部有哪些安全控制来保护暴露给用户的管理接口（基于 Web 的、API 等）

√ 在使用云提供商提供的任何 VM 镜像（image）或模板前，验证它们的完整性及出处。

√ 必须使用嵌入 hypervisor API 的 VM 定制的安全机制对 VM 背板上的流量进行细粒度的监测，这些流量对传统的网络安全控制设备来说是不可见的。

√ 虚拟操作系统的管理员访问控制是极为重要的，应采用与企业身份管理集成的强认证以及防篡改的日专和完整性监测工具。

√ 探究 VM 分段的可行性和有效性，根据使用类别、产品阶段（如开发、生产和测试）和服务器、存储等不同物理硬件上的数据敏感度生成不同的安全域。

√ 具有报告机制以提供隔离的证据，并在隔离被破坏时产生告警。

√ 对于通过管理手段保证 VM 间隔离的多租户情形要特别留意，有些情况下可能有隔离方面的监管要求。

贡献者: Bikram Barman, Girish Bhat, Sarabjeet Chugh, Philip Cox, Joe Cupano, Srijith K. Nair, Lee Newcombe, Brian O'Higgins

Copyright © 2010 Cloud Security Alliance

参考资料

A guide to security metrics. SANS Institute, June 2006. http://www.sans.org

Amazon EC2 API - http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/

Amazon Elastic Compute Cloud Developer Guide, http://docs.amazonwebservices.com/AWSEC2/2009-03-01/DeveloperGuide/

Amazon Simple Queue Service Developer Guide, http://docs.amazonwebservices.com/AWSSimpleQueueService/2008-01-01/SQSDeveloperGuide/

Amazon Simple Storage Service Developer Guide, http://docs.amazonwebservices.com/AmazonS3/2006-03-01/

Amazon SimpleDB Developer Guide, http://docs.amazonwebservices.com/AmazonSimpleDB/2007-11-07/DeveloperGuide/

Amazon web services blog: Introducing amazon virtual private cloud (vpc), Amazon, August 2009. http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html

Amazon Web Services: Overview of Security Processes, September 2008

An Innovative Policy-based Cross Certification methodology for Public Key Infrastructures. Casola V., Mazzeo A., Mazzocca N., Rak M. 2nd EuroPKI Workshop. Springer-Verlag LNCS 35. Editors: D. Chadwick, G. Zhao. 2005.

Auditing the Cloud, Grid Gurus, http://gridgurus.typepad.com/grid_gurus/2008/10/auditing-the-cl.html, October 20, 2008

Azure Services Platform, http://msdn.microsoft.com/en-us/library/dd163896.aspx

Balanced Scorecard for Information Security Introduction", Published: March 06, 2007, http://technet.microsoft.com/en-us/library/bb821240.aspx

BITS Kalculator and BITS Financial Services Shared Assessments Program (third party provider assessment methodology)

Building Security In Maturity Model, http://www.bsi-mm.com/

Business case for a comprehensive approach to identity and access management, May 2009 https://wiki.caudit.edu.au/confluence/display/CTSCIdMWG/Business+case

Business Roundtable, Principles of Corporate Governance, 2005

Business Roundtable, Statement on Corporate Governance, 1997.

Business Software Alliance, Information Security Governance: Towards a Framework for Action Centers for Medicare and Medicaid Services Information Security Risk Assessment Methodology

Cloud Computing and Compliance: Be Careful Up There, Wood, Lamont, ITWorld, January 30, 2009

Cloud computing definition, by P. Mell and T. Grance, NIST June 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Cloud Computing is on the Up, but what are the Security Issues?, Mather, Tim, Secure Computing Magazine (UK), March 2, 2009.

Cloud Computing Use Case Group Whitepaper -http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing vocabulary (cloud computing wiki) http://sites.google.com/site/cloudcomputingwiki/Home/cloud-computing-vocabulary

Cloud Computing: Bill of Rights, http://wiki.cloudcomputing.org/wiki/CloudComputing:Bill_of_Rights

Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum, V 1.0, April 2009

Cloud Security and Privacy – An Enterprise perspective on Risks and Compliance from O'Reilly - http://oreilly.com/catalog/9780596802776/ -

Cloud Standards Organization - http://cloud-standards.org/

Cloud Storage Strategy, Steve Lesem, July 19, 2009, http://www.cloudstoragestrategy.com/2009/07/cloud-storage-and-the-innovators-dilemma.html

Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (DRAFT), 2009. http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf

Contracting for Certified Information Security: Model Contract Terms and Analysis (published by the Internet Security Alliance and available at www.cqdiscovery.com)

Contracting for Information Security: Model Contract Terms (published by the Internet Security Alliance and available at www.cqdiscovery.com)

CPMC ClearPoint Metric Catalog, 2009 Online Available: http://www.clearpointmetrics.com/newdev_v3/catalog/MetricApplicationPackage.aspx

CVSS A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007 Online Available: http://www.first.org/cvss/cvss-guide.html

Data Lifecycle Management Model Shows Risks and Integrated Data Flow, by Ernie Hayden, Information Security Magazine, July 2009
http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321704_mem1,00.html

Data Privacy Clarification Could Lead to Greater Confidence in Cloud Computing, Raywood, Dan, Secure Computing Magazine (UK), March 9, 2009.

Defending Electronic Mail as Evidence—The Critical E-Discovery Questions, Jeffrey Ritter, (available at www.cqdiscovery.com)

Does Every Cloud Have a Silver Compliance Lining?, Tom McHale, July 21, 2009 Online Available: http://blog.ca-grc.com/2009/07/does-every-cloud-have-a-silver-compliance-lining/

Encryption of Data At-Rest: Step-by-step Checklist", a whitepaper prepared by the Security Technical Working Group of the Storage Network Industry Association (SNIA).

ENISA - http://www.enisa.europa.eu/

Fedora Infrastructure Metrics, 2008. http://fedoraproject.org/wiki/Infrastructure/Metrics

Few Good Information Security Metrics, By Scott Berinato, July 2005 Online Available: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Force.com Web Services API Developer's Guide, http://www.salesforce.com/us/developer/docs/api/index.htm

Global Privacy & Security, Francoise Gilbert, (Aspen Publishing 2009).

GoGrid API - http://wiki.gogrid.com/wiki/index.php/API

GSA to launch online storefront for cloud computing services, August 2009. http://www.nextgov.com/nextgov/ng_20090715_3532.php

Guidelines for Media Sanitization," NIST's Special Publication 800-88

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, T. Ristenpart, et al,

http://blog.odysen.com/2009/06/security-and-identity-as-service-idaas.html

http://blogs.forrester.com/srm/2007/08/two-faces-of-id.html

http://blogs.intel.com/research/2008/10/httpseverywhere_encrypting_the.php

http://code.google.com/apis/accounts/docs/AuthForWebApps.html

http://code.google.com/apis/accounts/docs/OpenID.html

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

http://csrc.nist.gov/publications/PubsSPs.html

http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

http://www.aspeninstitute.org/publications/identity-age-cloud-computing-next-generation-internets-impact-business-governance-socia

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

http://www.sas70.com

https://siswg.net/index.php?option=com_docman&task=cat_view&gid=21&Itemid=99999999

Information Security Governance: A Call to Action, National Cyber Security Summit Task Force, Corporate Governance Task Force Report, April 2004.

Information Security Law: Emerging Standard for Corporate Compliance, Thomas Smedinghoff, (ITGP 2008).

ISACA, IT Governance Institute, Control Objectives for Information and related Technology (CobiT), 4.1

ISO/IEC 19011:2002 Guidelines for quality and/or environmental management systems auditing

ISO/IEC 20000-1:2005 Information technology—service management—Part 1: Specification

ISO/IEC 20000-1:2005 Information technology—service management—Part 2: Code of practice

ISO/IEC 21827:2008 Information technology—Systems Security Engineering—Capability Maturity Model (SSE-CMM®)

ISO/IEC 27000:2009 Information technology—Security techniques—Information security management systems—Overview and vocabulary

ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements.

ISO/IEC 27002:2005 Information technology—Security techniques—Code of practice for information security management

ISO/IEC 27005:2008 Information technology—Information security techniques—Information security risk management

ISO/IEC 27006:2007 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 28000:2007 Specification for security management systems for the supply chain

ISO/IEC 38500:2008 Corporate governance of information technology

IT Governance Institute, Board Briefing on Governance, 2nd Edition, 2003

IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006

ITGI Enterprise Risk: Identify Govern and Manage IT Risk—The Risk IT Framework, Exposure Draft version 0.1 February 2009.

Jericho Forum - http://www.opengroup.org/jericho/ and the Jericho Cloud Cube model http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Justify Identity Management Investment with Metrics, by Roberta J. Witty, Kris Brittain and Ant Allan, 23 Feb 2004. Gartner Research ID number TG-22-1617.

Managing Assurance, Security and Trust for Services. Online. Available: http://www.master-fp7.eu/

National Association for Information Destruction Inc - http://www.naidonline.org/forms/cert/cert_program_us.pdf

NIST Guidelines for Media Sanitization (800-88) - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

NIST Recommended Security Controls for Federal Information Systems (SP800-53)

NIST SP 800-30 Risk Management Guide for Information Technology Systems

OATH- http://www.openauthentication.org

OCEG, Foundation Guidelines Red Book, v1 10/27/2008

OCTAVE-S Implementation Guide, Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody, Version 1, 2005

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Open Cloud Computing Interface Working Group - http://www.occi-wg.org/doku.php

Open Security Architecture Group - http://www.opensecurityarchitecture.org

OpenCrowd - http://www.opencrowd.com/views/cloud.php

OpenID – http://openid.net

Copyright © 2010 Cloud Security Alliance

OpenID attribute exchange http://openid.net/specs/openid-attribute-exchange-1_0.htmlOAuth (created by a small group of individuals) http://OAuth.net/

OpenSocial – sharing social networking information http://www.opensocial.org/

ORCM Overcoming Risk And Compliance Myopia, August 2006 Online Available: http://logic.stanford.edu/POEM/externalpapers/grcdoc.pdf

OSAG Security Landscape - http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape

OWASP Top Ten Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Princeton Startup Lawyer, "Company Formation-Fiduciary Duties (the basics)", June 17, 2009, http://princetonstartuplawyer.wordpress.com/2009/06/17/company-formation-fiduciary-duties-the-basics/

Python Runtime Environment, http://code.google.com/appengine/docs/

Rackspace API - http://www.rackspacecloud.com/cloud_hosting_products/servers/api

Sailing in Dangerous Waters: A Director's Guide to Data Governance, E. Michael Power & Roland L. Trope, (American Bar Association, 2005).

SAML- http://www.oasis-open.org/specs/index.php#saml

Security Guidance for Critical Areas of Focus in Cloud Computing, Version 1, by Cloud Security Alliance, April 2009

Service Level Agreements: Managing Cost and Quality in Service Relationships, Hiles, A. (1993), London:Chapman & Hall

SNIA Encryption of Data At Rest: A Step-by-Step Checklist http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/ssif/knowledge_center/white_papers/Encryption-Steps-Checklist_v3.060830.pdf

SNIA Introduction to Storage Security http://www.snia.org/forums/ssif/knowledge_center/white_papers/Storage-Security-Intro1.051014.pdf

SNIA Storage Security Best Current Practices http://www.snia.org/forums/ssif/forums/ssif/programs/best_practices/

Storage Security Best Current Practices (BCPs)" by the Security Technical Working Group of SNIA

Sun Project Kenai API - http://kenai.com/projects/suncloudapis

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management—Integrated Framework (2004).

The Darker Side of Cloud Computing, by Matthew D. Sarrel, PC Mag.com, February 1, 2009

Copyright © 2010 Cloud Security Alliance

The Force.com Workbook, http://wiki.developerforce.com/index.php/Forcedotcomworkbook

The Institute of Internal Auditors, Critical Infrastructure Assurance Project, “Information Security Governance: What Directors Need to Know”, 2001

The International Grid Trust Federation (IGTF). http://www.igtf.net

United States General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, 1999.

United States Sentencing Commission, Guidelines Manual

vCloud API - http://www.vmware.com/solutions/cloud-computing/vcloud-api.html

Where We’re Headed: New Developments and Trends in the Law of Information Security, Thomas J. Smedinghoff, Privacy and Data Security Law Journal, January 2007, pps. 103-138

Windows Azure SDK, http://msdn.microsoft.com/en-us/library/dd179367.aspx

Windows Cardspace - http://msdn.microsoft.com/en-us/library/aa480189.aspx

WS-Federation : http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html